FAA SE-2020 SIR2FO
Contract: DTFAWA-10-D-00030
Task Order: 0024 System Engineering Manual Revision and Update
CDRL #: 0008
(30_0024_1207_0008_20121110)

Final Version of SEM (v4.0)

Submitted by:

Booz | Allen | Hamilton
8283 Greensboro Drive
McLean, VA 22102

Date: November 09, 2012

This document satisfies the delivery of CDRL 30_0024_1207_0008_20121110, ‘draft’ Final Version of SEM, version 4.0.

All thirty-two chapters received a separate qualitative and contextual edit before combining them all into a single, cohesive document.

This version of the SEM represents the content provided by the SEM Team and stakeholders to date. However, major aspects of SEM workshops were unable to be incorporated into this version of the SEM.

These aspects include the following:

- “System of Systems” as a theme that runs through chapters
- DOORS to SEM as a theme
- Make the SEM dynamic
- I2I Capture Teams
- Add an appendix on how to create certain SE tools
- Update all graphics

Therefore, the recommendation to FAA is to continue the revision of the SEM in order to realize the findings and recommendations of the workshops.

Federal
Aviation

on

Federal Aviation Administration
Systems Engineering Manual

November 9, 2012

Version 4.0

Version History

Version	Date published	Notes
4.0a	10 September 2012	First draft of revision and update. Edited by David J. Gannon.
4.0	9 November 2012	Final draft of revision and update. Worked in changes from workshops. Edited by David J. Gannon

This page intentionally left blank.

Table of Contents

.

1 – Introduction

Background

In September 2008, in a report entitled "*Identifying the Workforce to Respond to a National Imperative - The Next Generation Air Transportation System (NextGen)*," the National Academy of Public Administration called for the improvement of systems engineering competencies within the Federal Aviation Administration (FAA). Since the existing National Airspace System (NAS) Systems Engineering Manual (SEM) was last updated in 2006, this rewrite and revision of the NAS SEM is one of many improvements to the systems engineering competencies within the agency.

Systems engineering is still rather a young discipline and there have been many new developments over the past decade, including the revisions to many systems engineering standards and best practices. The agency appointed a team of systems engineers to develop a rewritten SEM based on these industry best practices and standards. This team held some of the highest industrial credentials in systems engineering (*e.g.*, INCOSE's Certified Systems Engineering Professional, INCOSE's Expert Systems Engineering Professional, and the Project Management Institute's Project Management Professional certifications) and academic degrees in systems engineering, as well as decades of experience in various government agencies.

The SEM team reviewed many other systems engineering manuals within federal and state governments to determine an accepted approach for a systems engineering manual. Rather than attempting to be some type of systems engineering textbook or standard operating procedures manual, good systems engineering manuals lay out what best practices and standards should be followed by the agency. These manuals are followed with plans, guidelines, templates, and procedures to implement the documented best practices. In other words, the SEM needs to define what systems engineering practices FAA should follow, and then proceed with how the agency agrees to accomplish it.

Purpose

The systems engineering practices and processes defined in the SEM are the best practices that FAA should strive to reach in order to accomplish NextGen.

Accordingly, the SEM is a guiding document for the development of training classes within FAA, but is not a training tool itself. Neither is the SEM a systems engineering textbook or standard operating procedures manual. Anyone who wants more information on any identified systems engineering process or practice is directed to an appropriate textbook, and some suggestions are offered within this SEM.

Furthermore, the SEM is not a policy document, although it is possible and preferred that policy is put in place to adhere to the SEM. Therefore, it does not define the Acquisition Management System (AMS) but rather explains what systems engineering practices should take place during the phases of AMS.

Audience

At a high level, the audience for the SEM includes members of Congress, the Office of the Inspector General, Office of Management and Budget (OMB), and FAA and other executives. The SEM indicates to these executives what systems engineering practices and processes FAA is striving to follow in order to accomplish the NextGen initiative.

Another audience for the SEM is academia and contractors who want to work with FAA.

FAA's senior systems engineers can use the SEM to know what processes the agency has adopted. However, these senior systems engineers should know how to follow the processes without instructions from the SEM. Junior systems engineers should always have senior systems engineers mentors, and the SEM describes what practices these junior systems engineers should become proficient in or learn.

Contents

The SEM is divided into four groups, the Technical Management Processes, the Technical Processes, the AMS phases, and the Specialty Engineering processes.

The program manager uses the Technical Management Processes (Figure 1-1) to manage the technical development of the system increments, including the supporting or enabling systems. The Technical Management section discusses the eight technical management processes that are used throughout the life cycle.

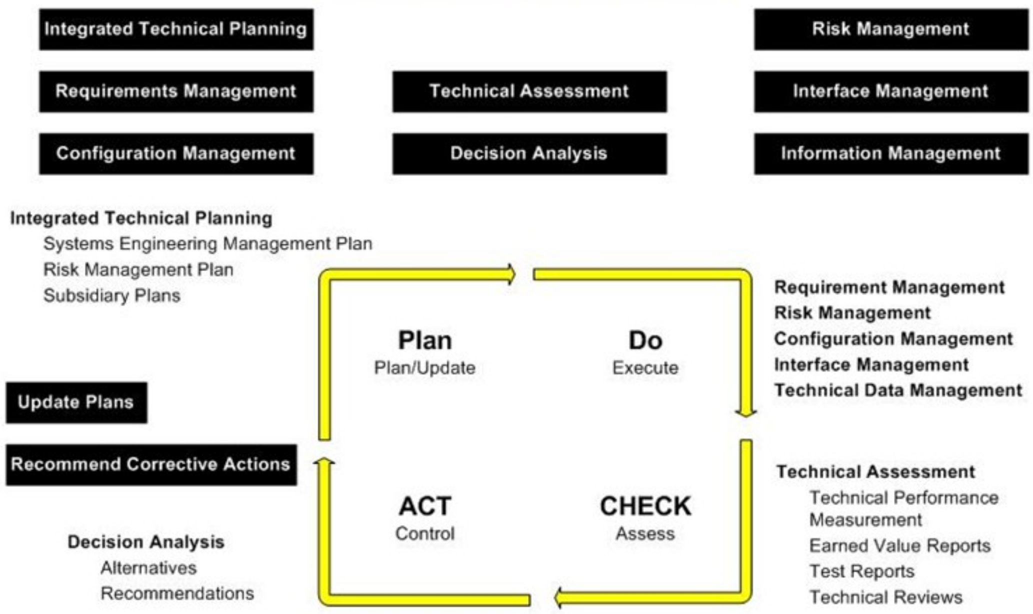


Figure 1-1. Technical Management Processes

The Technical Processes (Figure 1-2) are used to define the requirements for a system, to transform the requirements into an effective solution via design specifications, to permit consistent reproduction of the solution where necessary, to use the solution to provide the required services, to sustain the provision of those services and to dispose of the solution when it is retired from service (ISO-15288 2008). The Technical Process chapters adhere to the concepts outlined in (ISO-15288 2008) and expanded upon in (IEEE 1220 2005). It is expected that these three processes are iterative.

Consequently, the technical processes similarly follow the V-model, as depicted in figure 2. The V-Model is a systems development model to define a uniform procedure for product or project development. Nonetheless, it is expected that these processes are iterative. The only constraint is Operational Concept must start before Functional & Performance Allocation, which in turn must start before Design Solution. However, it is expected (and probably desirable) to return to an earlier process based on later findings. As for Validation, there is an early and an end-product validation. Also there is an early verification, which is sometimes called traceability of requirements, and a product verification.

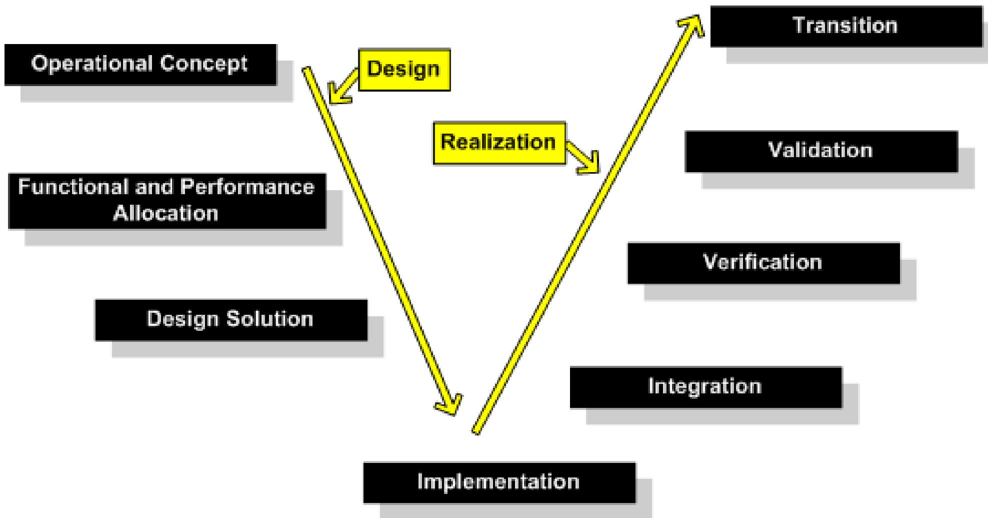


Figure1-2. Technical Processes

The AMS lifecycle section describes the phases that a needed product goes through from identification of the stakeholder need to use of that product in the operational environment. The AMS lifecycle chapters also indicate what systems engineering processes and practices, as described elsewhere in the SEM, should be addressed in each phase of the Acquisition Management System (Figure). The SEM chapters correspond to the phases of Service-Gap Analysis, Concept and Requirements Definition (CRD), Initial Investment Analysis – IIA, Final Investment Analysis – FIA, Solution Implementation, and In-Service Management.

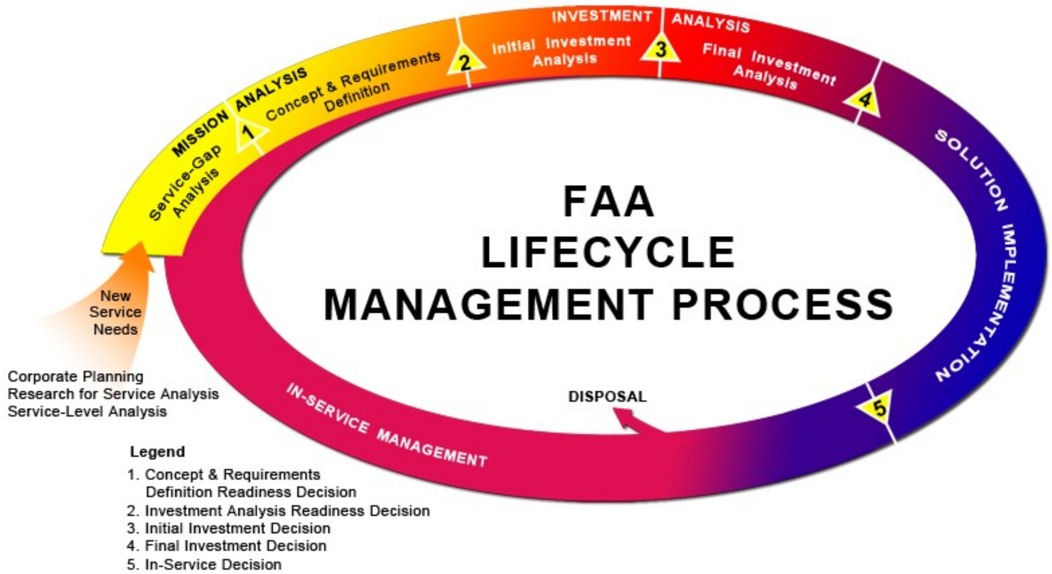


Figure 1-3. The AMS Processes

Service-gap analysis is the first phase in the AMS life cycle. It relates to the Operational Concept technical process. Service-gap analysis is conducted in response to a priority service need within an EA Roadmap that is vital to the FAA accomplishing its overall mission. For such needs, service-gap analysis develops a qualitative preliminary description of the priority need, existing legacy assets, capability shortfall, and develops the Concept and Requirements Definition Plan.

Concept and Requirements Definition is the second phase within the AMS life cycle. In this phase, the Operational Concept technical process is furthered and the Functional and Performance Allocation is initiated. The primary goals of concept and requirements definition are to translate priority service needs from an Enterprise Architecture roadmap into preliminary requirements and a Solution Concept of Operations (CONOPS), and to identify and define the most promising alterative solutions deemed best able to satisfy the priority service need efficiently and effectively.

Investment analysis is the third phase, and begins with the investment analysis readiness decision, which determines whether the detailed shortfall analysis, solution CONOPS, preliminary requirements, and initial alternatives are sufficiently defined to warrant entry into investment analysis. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery. Investment analysis consists of two stages. The Initial investment analysis generates the information needed to select the alternative offering the most promising solution to the service shortfall. The Final investment analysis develops preliminary planning and an acquisition program baseline for the alternative selected at the initial investment decision.

The fourth phase of the AMS life cycle, the Solution Implementation phase begins with the final Investment decision, during which an acquisition program is established for the solution selected and ends when the new capability goes into service (i.e., when a new service or capability is commissioned into operational use at all sites).

In-service management is the fifth and final phase of the AMS Lifecycle and involves two distinct sets of work activities. The first set monitors and assesses real-world performance of operational assets against baseline requirements and expected benefits, and takes action to optimize performance throughout their operational life. The second set of activities operates and maintains operational assets and their physical and support infrastructure throughout their service life.

Finally, the Specialty Engineering processes are the engineering domains that are not typical of the main engineering effort but are equally important. In the SEM, the Specialty Engineering processes are Reliability, Maintainability, and Availability (RMA); Life Cycle Engineering; Electromagnetic Environmental Effects and Spectrum Management; Human Factors Engineering; Information Security Engineering; System Safety Engineering; Hazardous Materials Management and Environmental Engineering; and Special Considerations for Systems of Systems.

2 – Process Management

Introduction

Process Management is a holistic management approach that promotes process effectiveness and ensures that all planned and systematic activities associated with those processes fulfill stakeholder needs and are of the highest quality. Process Management encompasses Quality Management, Business Process Management, and Business Process Reengineering. Process Management is committed to delivering quality products and services through the implementation of well managed project processes. A project process is a collection of related tasks and activities meant to produce a specific goal in the form of a service or product. They are used to plan, execute, monitor and control project activities to provide maximum benefits to the stakeholder and help achieve organizational and mission objectives. Process Management considers project processes to be strategic assets to any project. It stresses the importance of sufficiently understanding, managing, and continuously improving these processes to produce value added products and services to the stakeholder.

Within FAA, there are eight project processes, also referred to as the technical management processes. These processes are iterative and may be implemented with as much rigor and formality as needed. The eight technical management processes are:

1. Integrated Technical Planning
2. Requirements Management
3. Interface Management
4. Risk Management
5. Configuration Management
6. Information Management
7. Technical Assessment
8. Decision Analysis

FAA can use either ISO (International Organization for Standardization) or FAA iCMM (integrated Capability Maturity Model) to implement improvements to the project processes during the project lifecycle. ISO 9001 provides a set of business process activities to ensure stakeholder satisfaction is achieved. The iCMM model was designed by FAA and it describes characteristics for assessing efficient internal FAA processes. The FAA iCMM can be used by any organization pursuing process improvements. The practices in the iCMM have been integrated from 10 sources, including ISO 9001.

Whether ISO 9001 or iCMM is used, a Quality Management System (QMS) must be in place throughout an FAA project's lifecycle. A QMS is a management system that directs, measures, controls, and improves products and services. It has defined policies, processes, and procedures that define core business functions. ISO 9001 is the international standard for Quality Management systems. The FAA iCMM quality focus is to ensure the quality of the product or service, ensure the quality of the processes to generate or provide the product, and provide management visibility into the processes and products. Both can be used to determine if quality is met. While FAA can select the QMS to be used for the government activities related to a project, the contractor is required to satisfy the contract specifications regarding a quality system. In general, the government can require that the contractor have a QMS, but not the specific QMS to be used.

For the purposes of this manual, the PDCA (Plan-Do-Check-Act) management method will be used to describe each technical management process as well as demonstrate the relationship between the processes. PDCA, also known as the Deming circle or Shewhart cycle, is a four-step, iterative model used for continuous improvement; developing new or improved processes, products, or services; implementing change; or prioritizing and analyzing problems and root causes. PDCA was selected as the management modeling method for the technical management processes because it demonstrates the iterations of the individual processes and the importance of continuous process improvements. The PDCA cycle is depicted in Figure 2-1.

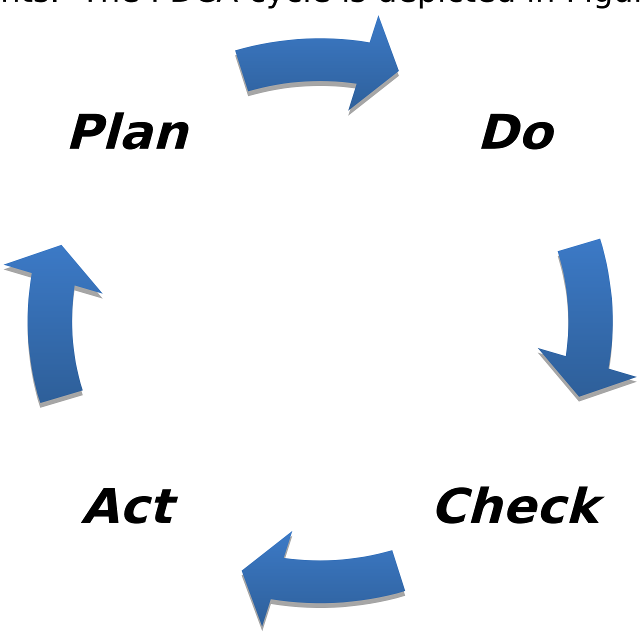


Figure 2-1. Plan-Do-Check-Act Cycle

Each phase in the PDCA cycle is explained below. In each one, the chapters of the SEM that relate directly to that phase are listed.

Step 1: PLAN – Develop a Plan to Address the Identified Need

This is the preparation phase. Once a need has been identified, a plan is developed to address that need. This plan will describe, at a minimum, what needs to be done, how to do it and who should do what in order to satisfy the identified need and fulfill stakeholder expectations. This plan includes tasks lists, roles and responsibilities, and may even include cost and schedule specifics. After the plan is completed, it must be shared and communicated with all relevant stakeholders.

Chapter 3: Integrated Technical Planning Process
Chapter 3 describes the technical management process that occurs during the Plan phase of the PDCA cycle. Integrated Technical Planning addresses the creation of technical plans for FAA projects and lists the plans all projects should have, resulting in a Systems Engineering Management Plan (SEMP).

Step 2: DO – Implement the Plan

This is the implementation phase. It consists of implementing the plan created in Step 1: PLAN and then communicating the progress of the planned activities and tasks to all relevant stakeholders. This phase can be as easy or as difficult as the plan that was created.

Chapter 4: Requirements Management Process
Chapter 5: Interface Management Process
Chapter 6: Risk Management Process
Chapter 7: Configuration Management Process
Chapter 8: Information Management Process
Chapters 4-8 describe the technical management processes that occur during the DO phase of the PDCA cycle. All five chapters are project areas that are managed throughout the entire lifecycle.

Step 3: CHECK – Review the Actions Performed

This is the review phase. During this phase, the results from performing the plan are compared to the project objectives and planned results. Areas of success and areas of improvement are identified and communicated to all relevant stakeholders

Chapter 9: Technical Assessment Process
Chapter 9 describes the technical management process that occurs during the Check phase of the PDCA cycle. This chapter outlines the systems-engineering-related assessments that occur during the AMS lifecycle. These assessments check the project progress at specific points in the life cycle.

Step 4: ACT – Perform Changes Resulting from Step 3

This is the action phase. Any areas still needing improvement following the review during the Check phase are addressed here. Any necessary changes are incorporated and communicated to all relevant stakeholders resulting in the need being fulfilled.

Chapter 10: Decision Analysis Process

Chapter 10 addresses the issues surrounding a decision when two or more alternatives exist. When actions need to be taken, this section details the steps required to ensure that they result in the best solution.

Each project process will have its own PDCA with its own set of metrics, goals, targets, and initiatives, and will be described in more detail in its respective chapter. This PDCA model places FAA's technical management processes in a continuous-feedback loop so managers can ensure continuous process improvement.

Figure 2-2 depicts the relationship between the technical management processes and the PDCA cycle.

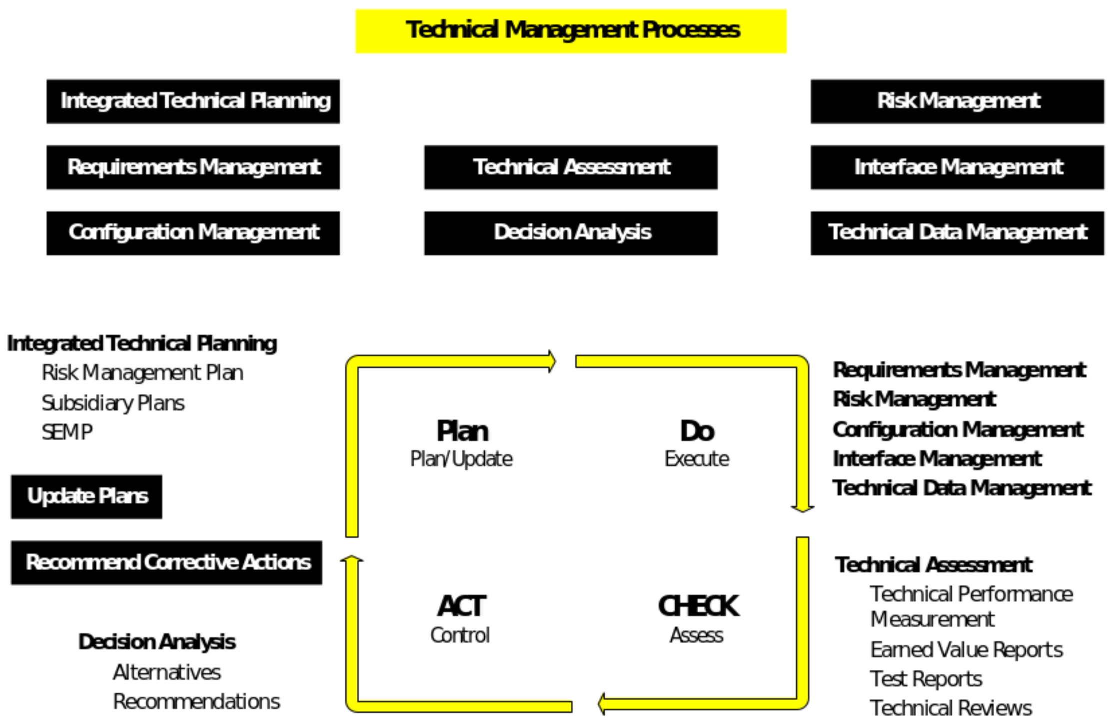


Figure 2-2. Plan-Do-Check-Act Cycle for Technical Management Chapters

The PDCA relates FAA's technical management processes to each other as well as the activities within each process. Process Management ensures continual process improvement and provides an environment capable of managing the complex systems associated with NextGen.

External Sources for More Detailed Information

For more information, see (Sage and Armstrong 2000)

For related information, see INCOSE Handbook, chapter 7.5: Quality Management Process

More information on the Pareto chart, including constructing one, can be found in (Blanchard and Fabrycky 1998)

This page intentionally left blank.

3 – Integrated Technical Planning

Introduction

Planning provides the basis for effective action and the ability to anticipate and prepare for changes that inevitably affect project progress. Planning determines in advance which tasks are needed to complete a project. Integrated Technical Planning determines those tasks that are needed to complete a project from a technical perspective. It provides the tactical and strategic means of defining problems, forecasting conditions, and coordinating a project's technical activities to provide superior products and services to the stakeholders.

A plan, at a minimum, contains the tasks to be done, when they need to be done, and who is responsible for doing them. Integrated Technical Planning provides guidance and tools to produce plans that address the technical scope of a project. These plans are called integrated technical plans or simple technical plans. Technical plans are used to track and monitor a project's progress as well as detail how the other systems engineering processes are applied throughout the life cycle.

Integrated Technical Planning occurs during the "Plan" phase of the PDCA cycle (Plan, Do, Check, Act) for the technical management processes. It provides the foundation for performing the other systems engineering process. Integrated technical planning is an iterative process and applies to all projects regardless of size, complexity, or status (*i.e.*, new or legacy).

The Integrated Technical Planning PDCA cycle is depicted in Figure 3-1. The primary outputs from this process are the Systems Engineering Management Plan (SEMP) and any supporting systems engineering plans not contained in the SEMP, including the OMB Circular 15, Exhibit 300, Attachment 3, Implementation Strategy and Planning (ISAP) document.

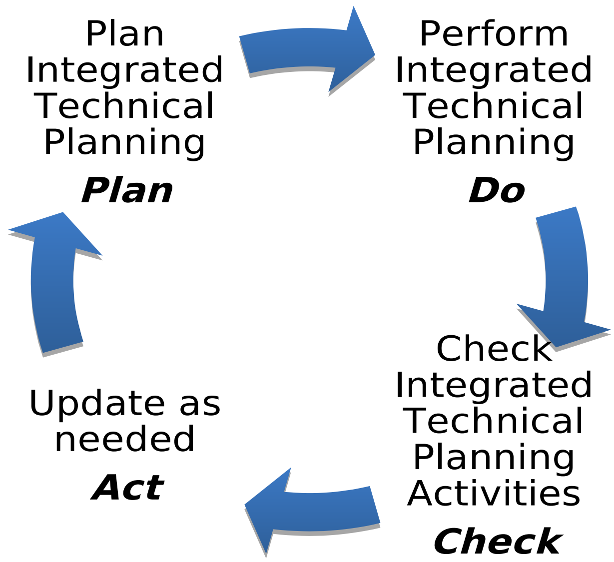


Figure 3-1. Integrated Technical Planning PDCA Cycle

Objective

The Integrated Technical Planning processes plans the technical work efforts required to satisfy organizational and mission needs.

Inputs or Essential Criteria

An input to the Integrated Technical Planning process is information that the Integrated Technical Planning process needs. This information either provides directions; is the basis for or otherwise drives Integrated Technical Planning process activities; or it requires action through one or more Integrated Technical Planning process tasks.

The primary inputs to the Integrated Technical Planning Process are:

- **FAA policy**. The specific applicable policies will vary project to project and the plan being developed
- **Planning Criteria**. Planning Criteria provides constraints and boundaries for the planning activities. Some examples of planning criteria are:
  - Requirements
  - Physical Architecture
  - Analysis Criteria
  - Concept of Operations (CONOPS)
  - Integrated Master Schedule
  - Corporate Strategy and Goals
  - Enterprise Architecture

Integrated Technical Planning Process Elements

PLAN: Plan Integrated Technical Planning

Preparing for the Integrated Technical Planning is important to successfully implementing the process, which subsequently results in the successful implementation of the other systems engineering processes.

The primary activity in the "PLAN" phase of Integrated Technical Planning is:

1. Develop an Integrated Technical Planning Strategy

Step 1: Develop an Integrated Technical Planning Strategy

The Integrated Technical Planning strategy outlines how integrated technical planning will be conducted for the project of interest in order to meet the project mission and needs. The Integrated Technical Planning strategy is developed in accordance with all available and applicable FAA policy and guidance documents for the project of interest. Each project will have an Integrated Technical Planning strategy that addresses that project's planning needs and will enable the Integrated Technical Planning process activities completed during the "DO" phase.

At a minimum, a good Integrated Technical Planning strategy should address the following:

- Identify all stakeholders
- Identify and gather Integrated Technical Planning inputs
- Assign roles and responsibilities for Integrated Technical Planning process activities
- Define format for Technical planning documents
- Define technical plans needed for project of interest
- Define schedule for Integrated Technical Planning process activities and updates
- Define criteria for technical updates and re-planning needs
- Establish communication plan with stakeholder
- Identify planning tool, when applicable

DO: Perform Integrated Technical Planning

Integrated Technical Planning prepares the technical plans and directs all the technical effort for the project of interest. These plans are maintained throughout the lifecycle. Performing integrated technical planning ensures more accurate costing of a project and significantly aids in successful project completion. The Integrated Technical Planning strategy is used to direct the process activities.

The Integrated Technical Planning process activities for the "DO" phase are:

1. Develop a SEMP
2. Develop any additional supporting plans, separate from the SEMP

Step 1: Develop a SEMP

The SEMP is the only implementing document that integrates all SE activities. It unambiguously ties together all systems engineering elements required to attain project objectives. It identifies and ensures control of the overall technical process. The SEMP helps project managers develop their systems engineering approach, providing a well thought-out and documented technical foundation for the project. It should be established early in the project life cycle and supports project management by defining comprehensive systems engineering activities, addressing both government and contractor technical activities and responsibilities.

The SEMP describes the program's overall technical approach, including systems engineering processes; resources; and key technical tasks, activities, and events along with their metrics and success criteria. The following steps shall be used to develop a SEMP.

Step 1.1 Collect Inputs

SEMP development relies on information from both technical and nontechnical documents. Inputs are also gathered from Screening Information Requests (SIR), Statements of Work (SOW), Integrated Master Schedules (IMS) and draft Implementation Strategy and Planning (ISAP) documents.

Step 1.2 Analyze Inputs

To determine the required SE effort to which the project manager has committed, review the ISAP that reflects the nature and magnitude of the project.

Step 1.3 Define Activities and Efforts

After evaluating all inputs, determine how to integrate activities. Decisions that should be made involve:

- Tailoring the SE processes
- Selecting an approach to ensure integration of engineering specialties
- Determining how project team members interact and communicate to execute technical program planning and control
- Identifying the explicit SE responsibilities, accountability, and authority, accounting for all planned tasks
- Developing the structure of the comprehensive SE inputs to the IMS (included in the ISAP) for schedule tasks

Step 1.4: Baseline

Prepare a draft SEMP for review and community, using input from all SE processes, enterprise management, and, when appropriate, the

stakeholders. More information on baselines is available in Chapter 7: Configuration Management.

Step 1.5: Interface with other SE processes

The SEMP interfaces with, and forms a roadmap to, any other SE and engineering specialty standalone plans. The SEMP should contain technical plans for each SE process.

Step 1.6: Update and Maintain the SEMP

IT is recommended that throughout the lifecycle of a project, SE monitors inputs, especially to the ISAP, and when there is a significant change in one or more inputs that the SEMP is updated to reflect the change.

There is no prescribed format for the SEMP. It may be a single plan or consist of multiple plans, depending on the project size and complexity. It contains planning for all SE processes that the project requires, including specialty elements.

At a minimum, the SEMP must include:

- An introduction that states the project purpose
- Work Breakdown Structure
- Technical Plans, as applicable to the project

Work Breakdown Structure

The Work Breakdown Structure (WBS) is a key element of planning. It lists the technical activities, a schedule of technical milestones, resources assigned to the technical aspects of a project, and cost estimates associated with the SE activities. It also contains the activity list, schedule, and criteria for all planned technical reviews.

The WBS is a deliverable-oriented grouping of project elements, which organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of a project component.

A well-developed WBS should be at least three to four levels deep, with each level five to nine elements broad.

Technical Plans

Each SE process will have a plan. Each plan must include a definition of the products, roles and responsibilities, and task completion schedule. Typical plans found in a SEMP are:

- Requirements Management Plan – details the total effort in managing requirements.
- Decision Analysis Plan – documents the formal management planning regarding how to assess in a fair and impartial manner alternative

solutions to a problem or design issue associated with a project product development

- Interface Management Plan – documents the formal management system of interface controls that ensures physical and functional compatibility between interfacing hardware, software, and facilities.
- Risk Management Plan – describes the approach, methods, procedures, and criteria for risk management and its integration into the program decision process.
- Configuration Management Plan – documents the formal CM management system to ensure that the integrity and continuity of the design, engineering, and cost tradeoff decisions made among technical performance, producibility, operability, testability, and supportability are recorded, communicated, and controlled by project and functional managers.

Step 2: Develop any additional technical plans, not contained in the SEMP.

In addition to the technical plans contained in the SEMP, there is additional planning that occurs during the life cycle and this planning is contained in standalone planning documents.

The most notable standalone plans are:

- Master Verification Plan
- Life Cycle Plan
- Exhibit 300, Attachment 3, Implementation Strategy and Planning Document

Each is described below.

Master Verification Plan (MVP)

A Master Verification Plan describes the overall verification program and provides the content and depth for full visibility of all verification activities. It describes and defines validation and verification planning as well as test and evaluation planning. This plan includes all the activities to ensure that the right system is being built and to confirm that evolving system solutions comply with functional, performance, and design requirements, as well as performance and characteristics of the delivered system. The systems engineer and verification engineer develop the plan with design and test organizations. Refer to Chapters 16: Verification and 17: Validation for additional information on these terms.

Life Cycle Plan

The Life Cycle Plan ensures that resources are available for all activities required for achievement of integrated life cycle support. It describes the tasks to perform life cycle activities and provides the content and depth of

detail necessary for full visibility of all life cycle activities. The plan fully defines each major activity and provides a general schedule and sequence of events. The plan includes the following planning sections: Deployment and Transition, Integrated Logistics, Real Property Management, Sustainment and Technology Evolution, and Disposal. Refer to Chapter 27: Life Cycle Engineering for additional information on these terms.

Implementation Strategy and Planning Document (ISAP)

The ISAP is the primary document within the AMS for planning the actions and activities to execute the project within the cost, schedule, benefits, and performance baselines. The ISAP includes both programmatic and selected SE planning elements. It is used to manage a project and contains the program Integrated Master Schedule, which includes milestones, accomplishments, and criteria. The ISAP relates tasks to program events and demonstrates logical, event-driven sequence of effort. It is directly traceable to the WBS, found in the SEMP, and facilitates resource planning; measures progress against planned efforts, ensures problem identification, and provides time-phased tasks and a framework to develop recovery and workaround plans.

CHECK: Check Integrated Technical Planning Activities

All technical plans developed for the project of interest are maintained and reviewed throughout the life cycle. Integrated Technical Planning is related to all of the SE processes, therefore the systems engineer and project manager must be aware of changes in other SE areas at all times, as they may necessitate revisions in the technical plans.

Some things to check for during the life cycle are:

- ✓ Have all Integrated Technical Planning process activities been performed according to the Integrated Technical Planning strategy?
- ✓ Have all Integrated Technical Planning process activities been performed correctly and completely?
- ✓ Are Integrated Technical Planning inputs still relevant and valid?
- ✓ Do the completed Integrated Technical Plans satisfy the entire project's planning needs?

ACT: Update as needed

This step of the Integrated Technical Planning PDCA cycle is reserved for making any changes to the Integrated Technical Planning process activities and associated work products. These changes mainly include updating the SEMP and other technical plans to reflect any changes that occur throughout the lifecycle including budget, schedule, or organizational changes, document revisions or planning software updates.

Outputs

The output of the Integrated Technical Planning process is the applicable technical plans for the project of interest. The planning is mostly contained within the SEMP, ISAP, and certain specialty domain plans.

Interdependencies

Every SE process is responsible for producing a technical plan, which details the task list, who will perform them and when for the project of interest. Therefore, this process is connected to all SE processes.

External Sources for More Detailed Information

For more information on preparing a WBS, schedules, and costs, see (Blanchard and Fabrycky 1998)
For one possible template for a formal SEMP on a large project, see (Sage and Armstrong Jr 2000, 483-484)
For a standard SEMP, see (IEEE 1220 2005).

References

Blanchard, Benjamin S, and Fabrycky, Wolter J. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

DAU. 2001. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Acquisition University Press, January.

DAU, Defense Acquisition University. 2010. 4 Systems Engineering. In *Defense Acquisition Guidebook*. Fort Belvoir, VA: Department of Defense, December 22. https://dag.dau.mil/Pages/Default.aspx.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

Sage, Andew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

This page intentionally left blank.

4 – Requirements Management

Introduction

The Requirements Management process manages all requirements and their associated artifacts for the project of interest. It is necessary throughout the entire life cycle, beginning from inception to disposal. Requirements Management is responsible for identifying any inconsistencies between the requirements, technical plans, and work product for the project of interest. It manages those requirements generated by the project, including both technical and nontechnical requirements, as well as those requirements received from the project stakeholders.

A **requirement** is an essential characteristic, condition, or capability that is to be met or exceeded by a system or component to satisfy standards, a contract, specification, or other formally imposed document. A requirements set is developed, documented, and baselined, when applicable, from the identified requirements. A **requirements set** is an aggregate set of requirements for a system that specifies its characteristics in totality. In FAA, requirements sets are contained in Requirements Documents (RD). There are several levels of RDs as well as several iterations, at the program level. The high-level "parent" requirements are contained in the NAS-RD, while program-level requirements can be found in the Program Requirements Document (PRD). Depending on where in the AMS lifecycle the project is, there can be an initial PRD (iPRD) and a final PRD (fPRD). More information on the AMS lifecycle phases are in Chapters 19-24. The System Specification Document (SSD) is used by the Contractor to finally build the system. All of these documents should be traceable and verifiable.

The Requirements Management process occurs during the "DO" phase of the PDCA (Plan, Do, Check, Act) cycle for the Technical Management processes. It is an iterative process and applies to all projects regardless of size or complexity. The Requirements Management process is tightly coupled with the 8 SE Technical Processes, more specifically, Operational Concepts (Chapter 11), Functional and Performance Allocation Process (Chapter 12), and Design Solution Process (Chapter 13), which details the development process of requirements and specifications.

The Requirements Management PDCA cycle is depicted in Figure 4.1. The outputs of this process are well managed requirements documents.

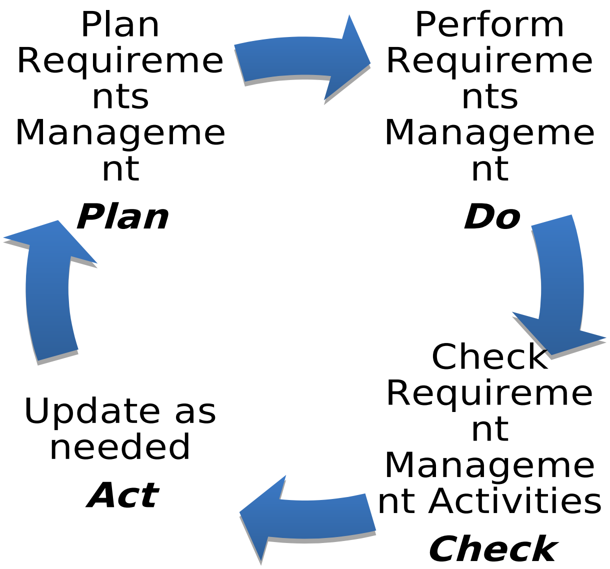


Figure 4-1. PDCA Cycle for Requirements Management

Objective

The Requirements Management Process maintains all requirements, requirements changes, and traceability between requirements throughout the project life cycle.

Inputs

An input to the requirements management process is information that the requirements management process needs that provides directions; is the basis for or otherwise drives requirements management process activities; or requires action through one or more requirements tasks.

The primary inputs to the Requirements Management Process are:

- FAA Policy
- Standards
- Corporate strategy and needs
- NAS Enterprise Architecture
- SEMP
- Functional and Physical Architecture
- Constraints
- Decision Analysis reports
- IRDs, ICDs
- Analysis Criteria
- Stakeholder Expectation Documents
- Baslines, Baseline Changes
- Validation Reports,
- Verification Requirements Traceability Matrix (VRTM)

- Risk Mitigation Plans

Requirements Management Process Elements

PLAN: Plan Requirements Management

Requirements Management process activities must be planned, before they are performed. Developing a Requirements Management Plan provides the basis for ensuring application of effective and efficient Requirements Management practices throughout the lifecycle. The Requirements Management plan is usually found the SEMP for the project of interest, but may also be a standalone document. It is the only task required to plan Requirements Management and is used to direct the Requirements Management process activities

Requirements Management Planning Activities:

1. Develop a Requirements Management Plan

Step 1: Develop a Requirements Management Plan

A Requirements Management Plan details the total effort in managing requirements for the project of interest.

At a minimum, a good Requirements Management Plan should address the following:

- Identify stakeholders
- Identify and gather inputs
- Establish criteria for distinguishing appropriate requirements providers
- Establish criteria for evaluation and acceptance of requirements
- Document list of requirements to be managed
- Establish Requirements Management Schedule
- Assign roles and responsibilities for requirements management activities
- Establish requirements verification and validation approaches
- Select a Requirements Management Tool, when applicable
- Define Requirements Management Change process, if separate from CM
- Develop a Communication Plan with stakeholders

DO: Perform Requirements Management

Requirements Management ensures that the end products meet the needs and expectations of the stakeholders. It manages requirements beginning from the stakeholder expectation document, contained in the Concept of Operations (CONOPS), through the system-level specification. More information on the CONOPS is provided in Chapter 11: Operational Concepts. The Requirements Management Plan details how the requirements management activities will be performed for the project of interest.

The Requirements Management Process Activities are:

1. Gather requirements to be managed
2. Maintain requirements traceability
3. Validate and verify requirements
4. Manage requirements changes
5. Maintain consistency between requirements and all associated documentation

Each activity is described below.

Step 1: Gather requirements to be managed

Requirements are an integral part of any project and managing the correct requirements is imperative to the successful completion of the requirements management process. Using the criteria established in the Requirements Management Plan, the requirements that will be managed are gathered. Gathering only those requirements that satisfy the established criteria helps to decrease the possibility of requirements creep. **Requirements creep** is the continual and sometimes rapid growth of requirements during system development. Requirements Management provides check and balances against requirements creep and those requirements that are deemed “like-to-have” instead of “need-to-have” due to the repetitive review and approval that is required for the various RDs during the AMS lifecycle.

Upon completion of this step, there should be an agreed upon set of requirements with a shared understanding of those requirements amongst all stakeholders, internal and external to FAA, ready to be managed.

Step 2: Maintain Requirements Traceability

One of the major purposes of Requirements Management is to ensure traceability between user’s defined capabilities and needs and the sequence of serial requirements documents that identify and define system functional and performance requirements and maintain that traceability throughout the lifecycle. Requirements traceability allows the path of a requirement to be followed and described. It is used to capture the relationship between the requirements at all levels and guarantee that the final design satisfies all requirements. Requirements traceability can also be used to determine the origin on a specific requirement and the relationship between requirements across interfaces or other project artifacts. For detailed information on interfaces refer to Chapter 5: Interface Management. It helps to eliminate unnecessary or missing requirements by verifying that all requirements have a source. The requirements gathered in Step 1 should be developed in a way that allows for them to be traced back to its source as well as any related requirements (i.e. parents, children, peers). The traceability for a

specific requirement is determined during the requirements development process, however, it is the function of Requirement Management to ensure that the traceability is maintained.

A requirements traceability matrix can be used to help maintain requirements traceability throughout the lifecycle, a Verification Requirements Traceability Matrix is most commonly used in the FAA. **A Verification Requirements Traceability Matrix (VRTM**) is included as a part of every requirements and specification document. It provides information on the verification and traceability from a requirement to a higher level requirement or to its ultimate source. More on VRTM is provided in Chapter 16: Verification.

Step 3: Validate and Verify Requirements
All requirements must be both validated and verified. More information on Verification and Validation can be found in Chapter 16 and 17, respectively. From a Requirements Management perspective, however, the validating and verifying of requirements requires checking to make sure that the requirements being managed are written correctly to satisfy stakeholder needs. The requirements traceability matrix will be very useful in the validation and verification of a requirement.

A well written requirement must possess the following properties:

- Correct
- Unambiguous
- Complete
- Consistent
- Implementation-independent
- Traceable to documented statement(s) of need
- Traceable to evidence of the requirement's source
- Testable
- Verifiable
- Validatible
- Single-purposed (per requirement)

Some specific restrictions (to avoid ambiguity) include avoiding the use of "minimum" and "maximum" to state limits. Rather the use of "no less than" or "no greater than" is preferred. This restriction does not mean that the words "minimum" and "maximum" may not be used at all; it simply means that they should not be used to state limits.

Furthermore, vague, ambiguous, or general words and phrases are to be avoided. They include "flexible," "fault-tolerant," "high fidelity," "adaptable," "rapid" or "fast," "adequate," "user-friendly," "shall support," "shall allow,"

"shall enable," "shall maximize," "shall minimize," "shall provide," and "shall have the capability to" (SEM 2006) (INCOSE 2010). Although the phrase "shall provide" is debatably ambiguous, a better requirement would clarify what is meant by "provide." For example, the requirement, "the system shall display formatted data to the user," is definitely different from "the system shall store customized data on the client system." However, "the system shall provide data" could mean either of these requirements.

System requirements are documented in the formal "shall" language. This document must address the following five basic issues of a new or refreshed system (IEEE 830 1998):

1. Functionality – What is the system supposed to do?
2. External interfaces – How does the system interact with people and other system's hardware and software?
3. Performance – What is the speed, availability, maintainability, reliability, response time, recovery time of various functions, etc.?
4. Attributes – What is the portability, correctness, maintainability, security, etc. considerations?
5. Design constraints imposed on an implementation – Are there any required standards in effect, implementation language, policies for database integrity, resource limits, operating environment(s) etc.?

Step 4: Manage Requirements Changes

This activity manages and controls requirements changes throughout the life cycle, both before and after instituting formal configuration management, by using a defined change process, typically outlined in the Requirements Management Plan. The Configuration Management process establishes and maintains requirements baselines both during the requirements development process and after formal release of the requirements. The process also identifies and controls all issues and decisions, action items, formal and informal stakeholder directives, and any other real or potential changes to the requirements This activity is conducted according to the Configuration Management Process (Chapter 7: Configuration Management provides more information on this topic).

This change process is invoked when a new requirement is identified or a change occurs during any other activity within the Requirements Management process. The activity is a project wide, approved approach manages any and all changes to an identified requirement. It ensures that all involved stakeholders concur with the baselined requirement changes. This process also accounts for changes resulting from the Verification and Validation processes (Chapter 16 and 17 respectively). That is, if a test or other form of verification determines that a change in requirements is

necessary, the process ensures that the change process is initiated to accomplish the change.

Step 5: Maintain Consistency Between Requirements and Associated Documents

Maintaining consistency between requirements and their associated documents is an important part of the Requirements Management Process. As the requirements change, any and all related required and work products must also be updated to reflect the change. The requirements traceability matrix helps to identify which requirements and documents should be updated upon a requirement change. This task can be completed manually or automatically. The decision on which to use will be documented in the Requirements Management Plan.

There are a variety of mechanisms that can help organize requirements and their related information. Deciding which one to use depends on a variety of factors, including the size and complexity of the project, the number of requirements, and the budget. It is highly recommended that a secure and adaptable data repository or database be used to store, track, identify, and allow changes; to rank the changes; and to filter requirements and their traceable elements. Source documents and linkages to artifacts should also be maintained in the same database relative to the requirements.

The FAA standard tool for requirements management is the IBM Rationale Dynamic Object Orientation Requirements System (DOORS). The use of this tool helps to ensure that proper Configuration Management practices are administered as well as to keep derived requirements close to their documented sources.

It is recommended that the Requirements Management tools selected be capable of identifying and presenting the following types of information:

- **Requirements Documentation** – creating statements of requirements, status, requirement type, rationale, and history regarding each requirement, and presenting the requirements in an appropriate user-defined format
- **Traceability** – linking requirements to their parent, child, and peer requirements, resulting in user-defined, requirements-traceability matrices
- **Allocation** – linking requirements to the product hierarchy, resulting in user-defined, requirements-allocation documents
- **Verification** – linking requirements to specific verification approach attributes, resulting in requirements-verification and compliance documents

- **Traceability Impact Assessment** – assessing the impact of proposed changes to the requirement, product, and verification hierarchies
- **Compatibility** – communicating (minimum of import and export capabilities) with other automated tools

CHECK: Check all Requirement Management Activities

All the Requirements Management process activities and associated work products are reviewed during this phase of the Requirements Management PDCA cycle.

Requirements Management checklist to consider:

- ✓ Have all requirements management process activities been performed according to the Requirements Management Plan?
- ✓ Have all requirements management process activities been performed correctly and completely?
- ✓ Are requirements management process inputs still valid and relevant?
- ✓ Have all requirements changes been integrated?
- ✓ Have all requirements changes been communicated?
- ✓ Has traceability been maintained throughout the life cycle?
- ✓ Can all requirements documents be located and are they accessible to all stakeholders?

ACT: Update as needed

This phase of the Requirements Management PDCA cycle only occurs when changes need to be made to any of the process activities or associated work products following a formal or informal review. Those changes take place during this phase.

Outputs

The primary outputs of this process are well managed requirements documents and specification documents.

Interdependencies

Operational Concepts
Functional and Performance Allocation
Design Solution
Verification
Validation
Configuration Management
Integrated Technical Planning

References

DAU. 2001. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Acquisition University Press, January.

DAU, Defense Acquisition University. 2010. 4 Systems Engineering. In *Defense Acquisition Guidebook*. Fort Belvoir, VA: Department of Defense, December 22. https://dag.dau.mil/Pages/Default.aspx.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

This page intentionally left blank.

5 – Interface Management Process

Introduction

Interface Management helps to ensure that all the pieces of the system work together to achieve the system's goals and continue to operate together as changes are made to the system. FAA systems interoperate with a variety of other systems, platforms, humans, and system elements. These connections and relationships are generally known as interfaces. An interface is the performance, functional, and physical attributes required to exist at a common boundary. These interfaces must be precisely identified, controlled, and managed as early as possible and regularly throughout the system's life cycle.

Interface Management is crucial to successful and timely system development. As FAA moves closer to NextGen, the systems are becoming more complex and complex systems have many interfaces. Interface Management ensures that all facility and system interfaces are identified, any necessary interface requirements are clearly and completely defined, and that interfacing systems are designed to the same requirements. Interface Management also aids in resolving any incompatibility issues among interfaces and it reduces risk.

Interface Management occurs during the "DO" phase of the Plan-Do-Check-Act (PDCA) cycle for the Technical Management processes. Interface Management is an iterative process and occurs concurrently and in conjunction with other systems engineering processes. Interface Management can begin as soon as the mission need has been established.

The Interface Management PDCA cycle is depicted in Figure 5-1. The major outputs of Interface Management process are the Interface Requirements Document (IRD) and the Interface Control Document (ICD).

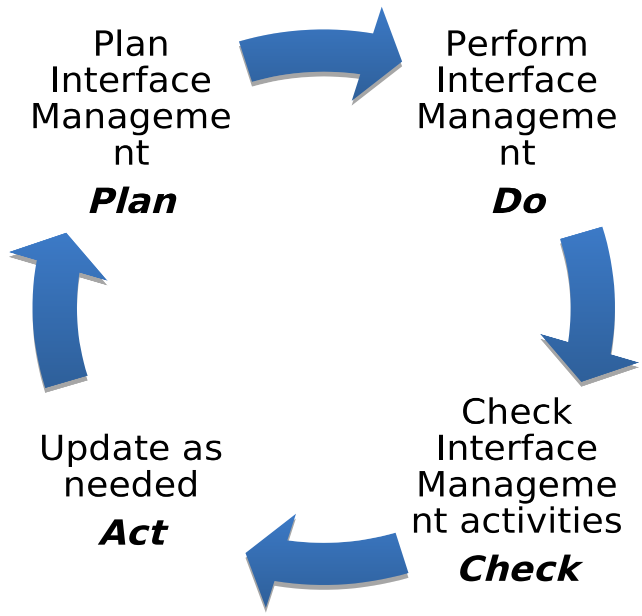


Figure 5-1. Interface Management PDCA Cycle

Objective

The Interface Management Process identifies, describes, and defines Interface Requirements to ensure compatibility between interrelated systems and between system elements. It also provides authoritative means of controlling the interface design.

Inputs

The primary inputs to the Interface Management Process are:

- CONOPS
- Enterprise Architecture
- Any relevant Requirements Documents (NAS RD, pPR, fPR)
- Trade study reports
- Physical and Functional Architecture
- SEMP, which contains the Interface Management Plan

Interface Management Process Elements

PLAN: Plan Interface Management

Preparing for Interface Management requires developing an Interface Management Plan, contained in the SEMP for the project of interest. The Interface Management Plan includes the Interface Control Planning section

that contains interface requirements and templates for preparing, revising, and processing ICDs unique to the project. The Interface Control Planning section also addresses supplier participation in the interface process.

At a minimum, a good Interface Management Plan should address the following:

- Provide the means for identifying, defining, documenting, and controlling the interfaces at all system levels
- Provide the means for changing the interfaces as required by the evolution of the design and for resolving interface incompatibilities
- Guide management, control, and documentation of all system functional and physical interfaces
- Establish the Interface Working Group (IWG) and its policies and procedure.
  - **Interface Working Group (IWG)**. IWG meetings serve two purposes: to ensure effective, detailed definition of interfaces by all cognizant parties, and to expedite baselining of initial Interface Requirements Documents (IRD), Interface Control Documents (ICD), and subsequent drawing changes by encouraging resolution of interface issues.
- Appoint IWG chairperson, who also functions as planning coordinator and is responsible for developing and establishing the policies and process for identifying, defining, documenting, auditing, and controlling interfaces
- Provide requirements and templates for preparing, revising, and processing the interface documentation; identifies products
- Establish the participants of the interface management process and their responsibilities
- Establish the interface management schedule

DO: Perform Interface Management

Interface Management includes the identification, definition, and control of all interfaces. It is responsible for making sure all the system elements work together to meet project goals and objectives. The Interface Management Plan, developed helps facilitate how the interface management process activities are conducted.

The Interface Management Process activities are as follows:

- Define the system boundary
- Define interfacing systems
- Identify interfaces
- Create Interface Requirements Document (IRD)

- Create Interface Control Document (ICD)

Each step is described below.

Step 1: Define the system boundary

At the beginning of a system's life cycle, the boundary or extent of the system being developed or modified must be established. This boundary defines the common interfaces between systems.

Step 2: Define Interfacing Systems

Once the system boundary has been defined, those systems that are currently co-functioning or will be co-functioning with the system being created or modified are defined. These systems can be internal or external to the new or modified systems.

- **Internal Interfaces** are those interfaces within the defined system boundary.
- **External Interfaces** are those interfaces outside the defined system boundary.

Steps 1 and 2 help identify and define which systems elements are under design control of the new/modified system. These steps also show the expected interactions among system elements under design control and external and/or high-level and interacting systems outside the system boundary.

Step 3: Identify Interfaces

After defining the system boundary and interfacing systems, the inputs and outputs flowing to and from the system across the interface boundary are next. These inputs and outputs contain the actual interfaces. Interfaces can be described functionally or physically.

- **Functional Interfaces** describe what the system is intended to do. It also includes subsystem functions as they relate to and support the system function. Functional interfaces clarify the functional responsibilities of the interfacing systems. Each interface has at least two associated functions.
- **Physical Interfaces** describe the composition and organization of the tangible system elements. They define and control the features, characteristics, dimensions, and tolerances of one design that affects another. Physical interfaces include material properties of the equipment that affect the functioning of mating equipment. They also include the system's operating system.

An N-squared (N^2) diagram is one example of a tool that can be used to determine the functional and physical interfaces. The N^2 diagram is a visual

matrix representing functional or physical interfaces between system elements. It is used as a systematic approach to identify, define, tabulate, design, and analyze functional and physical interfaces. It applies to system interfaces and hardware and/or software interfaces. Figure 5-2 is an example of an N^2 diagram.

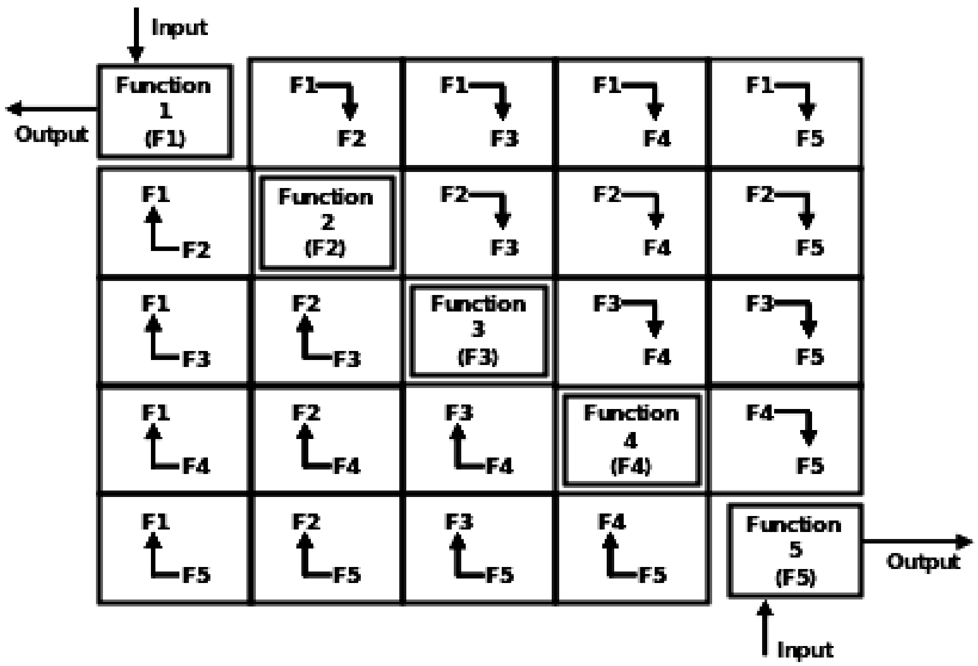


Figure 5-2. N^2 Diagram

Using tools such as N^2 diagrams to determine the functional and physical interfaces, these interfaces are documented. The functional interfaces identified in the functional N^2 diagram are documented in a Functional Interface list and the physical interfaces identified in the physical N^2 diagram are documented in a Physical Interface List.

Step 4: Create Interface Requirements Document (IRD)

The functional and physical interface lists developed in Step 3 are the primary input to the IRD. A set of interface requirements are generated from the list of physical and functional interfaces and are then documented in the IRD. The Interface Requirements Document (IRD) provides FAA with interface requirements between two elements, including type of interface (*e.g.*, electrical, pneumatic, hydraulic, etc.) and the interface characteristics (performance, functional, or physical). It must comply with the final Program Requirements Document (fPRD) for the project of interest. For more information on Configuration Management, refer to Chapter 7: Configuration Management.

- **Interface Requirements** specify the performance, functional, or physical attributes that are required to exist at a common boundary. This boundary can exist between two or more functions, systems, system elements, configuration items, or systems. This boundary was defined in Step 1. Interface Requirements shall be expressed in verifiable terms and follow the same formatting rules as system requirements. Refer to Chapter 4: Requirements Management for the characteristics of a good requirement.

Step 5: Create Interface Control Document (ICD)

The IRD is used to create the Interface Control Document (ICD). The ICD identifies the design solution to satisfy the interface requirements in the IRD. It describes the detailed, "as-built" implementation of the interface requirements. The ICD is usually developed by the vendor and must be in compliance with the IRD.

The IRD and ICD are the primary outputs of the Interface Management Process and both documents must undergo Configuration Management. For more information on Configuration Management refer to Chapter 7: Configuration Management.

Interface Management for Service-Oriented Architecture and Web Services

FAA's ongoing transition to the Next Generation Air Transportation System (NextGen) introduces a number of new advanced technologies and procedures. These bring into play new terminology and methodological approaches that require some readjustment in developing requirements and adaptation of specific inputs and outputs of the Interface Management process.

A key aspect of the transformation to the net-centric environment needed to achieve NextGen goals and objectives involves migration from systems that

interact in a point-to-point fashion to systems that are based upon the concepts of Service-Oriented Architecture (SOA). SOA is an architectural paradigm that supports service orientation as a way of thinking in terms of services, service-based development, and the outcomes provided by services. The special case of services that leverage Web and Internet-based technologies, known as Web services, are commonly used in FAA as a means of realizing SOA. (For more information about SOA and Web services, see FAA-STD-070 section 1.3 "Basic Concepts.")

Although adoption of SOA in FAA introduces many advantages (*e.g.*, platform and vendor diversity, use of open standards, reuse of existing assets, intrinsic extensibility, etc.), it also presents architects and developers with some challenges. When designing Web services, architects often have to provide highly specialized requirements for a loosely-coupled, standards-based, and platform-independent distributed system. Another task faced by developers of a SOA-based implementation is creation of a service description, which is the document that governs the mechanics of interaction between a service and its consumers by establishing the identity and functionality of the service, prescribing the service interface, and specifying the conditions for service invocation.

All these issues specific to service-based practices required adjustment of the existing interface management processes and resulted in two new documents explicitly tailored for Web service design and development: the Web Service Requirements Document (WSRD) and the Web Service Description Document (WSDD). These documents, which are designed to augment or replace IRDs and ICDs in the area of service-oriented development, are governed respectively by two Standard Practices: FAA-STD-070 Preparation of Web Service Requirements Documents and FAA-STD-065 Preparation of Web Service Description Documents.

In the context of the Interface Management Process for Web services the following substitutions are made: "WSRD" for "IRD" and "WSDD" for "ICD".

CHECK: Check Interface Management Activities

All the Interface Management process activities must be checked for completeness and accuracy, particularly the IRD and ICD or WSRD and WSDD, if applicable. The Interface Working Group (IWG) will be primarily responsible for checking these documents.

Interface Management checklist to consider:

- ✓ Ensure accuracy of interface definitions
- ✓ IRD satisfies the characteristics of a good requirement
- ✓ ICD compliance with IRD

- ✓ IRD compliance with fPRD
- ✓ Ensure all documents reflect any changes when design modifications occur or new requirements are added

ACT: Update the Interface Management Plan, IRD, and ICD

The “Act” phase of the Interface Management PDCA cycle is only necessary when changes to the interfacing systems, requirements, or design definition occur. When changes to either the IRD or ICD are needed the following activities are performed to implement those changes.

Interface Change Request Process for IRD and ICD.

Step 1: Prepare the interface change request and provide the following information:

- Description of the problem and the proposed change
- Analysis showing how the change solves the problem
- Analysis of how the change impacts system performance, effectiveness, and life cycle costs
- Analysis to ensure that the proposed solution does not introduce new problems
- Descriptions of resources and an estimate of the costs associated with implementing the change
- Statement of impact to system

Step 2: Provide change request to IWG, which shall determine if the authorized Interface Change Request (ICR) is within the scope. In-scope ICRs shall be returned to the ICR originator and the custodian of the IRD/ICD for preparation and release of an interface requirement. Out-of-scope ICRs shall be forwarded to the program manager.

Step 3: Coordinate draft IRD/ ICD with all affected organizations.

Step 4: Update IRD/ ICD upon approval and include the approved ICR.

Continue to perform the “Act” phase of the Interface Management PDCA cycle as needed.

Outputs

The IRD and ICD are the primary outputs of the Interface Management Process. Interface Management PDCA cycle allows for proper preparation of these documents and each phase of the cycle can be performed as needed.

Interdependencies

Integrated Technical Planning
Functional and Performance Allocation
Design Solution
Integration

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

6 – Risk, Issue, and Opportunity Management

Introduction

Risk, Issue, and Opportunity (RIO) Management is a significant part of the program management function. It focuses on identifying, assessing, controlling, and monitoring events throughout the life of a program/project/portfolio that may/will result in changes or impacts to program activities. From the mission analysis phase to the service life extension phase, RIO Management is a key activity in the FAA Acquisition Management System (AMS) life cycle. This section outlines the RIO Management framework, including high-level processes.

This section provides guidance for programmatic RIO Management. It does not address the processes for managing safety risks, occupational risks, security risks, hazards, and any other risks that are not directly related to a published program goal, e.g. cost, schedule, and/or technical goals. These other sources of risk have their own, specialized processes for identifying and managing related risks.

The PDCA (Plan, Do, Check, Act) cycle, depicted in figure 6.1, defines the full scope of RIO Management. The RIO Management process, figure 6.2, occurs during the "DO" phase of the PDCA cycle.

Figure 6-1. RIO Management PDCA Cycle

A **risk** is an uncertain event or situation with a realistic probability of occurring that has a negative impact to the successful accomplishment of

one or more project objectives. The following are some of the most common types of risks found in FAA projects and programs.

An **issue** is an event or situation that has occurred or is certain to occur and has a negative impact to the successful accomplishment of one or more project objectives.

An **opportunity** is an uncertain event or situation with a realistic probability of occurring that has a positive impact to the successful accomplishment of one or more project objectives.

Objective

The Risk, Issue, and Opportunity Management process identifies and analyzes the uncertainties of achieving project, program, or organizational objectives and develops plans to reduce the likelihood and/or consequence of those uncertainties.

Inputs

An input to the Risk, Issue, and Opportunity Management Process is information that the RIO process needs that provides direction; is the basis for or otherwise drives RIO process activities; or that requires action through one or more RIO tasks.

The primary inputs to the RIO Management PDCA Process are:

- FAA Policy
- Concept of Operations (CONOPS)
- SEMP
- Integrated Master Schedule
- Requirements Documents
- Analysis Criteria
- Constraints
- Standards

Risk, Issue, and Opportunity Management Process Elements

PLAN: Develop Risk, Issue, and Opportunity Management Plan

Planning for Risk, Issue, and Opportunity Management is essential to successfully implementing the RIO Management process. Although the process is iterative, the more upfront planning and preparation that occur,

the more effective the systems engineers and project managers will be at managing risks. Developing the RIO Management Plan is the major step required to implement RIO Management. The RIO Management Plan describes the approach, methods, procedures, and criteria for RIO management and its integration into project management.

At a minimum, a good RIO Management Plan should address the following:

- Relevant RIO management policies
- Relevant stakeholders
- Stakeholder Roles and responsibilities
- Relevant RIO management tools and techniques
- Process to perform RIO management
- Provide an avenue for evaluation and improvement of the RIO Management Activities
- Detailed plan outlining how the RIO management information will be captured, processed, and disseminated throughout the project life cycle

RIO Management Tools

The use of a RIO Management tool supports commonality and integration by allowing organizations to track and monitor RIOs, as well as giving management the appropriate exposure to all RIO data in a consistent manner. A tool also provides management with a consistent reporting capability/format to support their various needs, and allows RIO managers to efficiently manage RIOs on a day-to-day basis.

For Configuration Management (CM) purposes, a tool that can track RIO change history is important. This capability should track the full change history (change, date of change, and user who made the change) for each RIO. Reports can be generated by a tool to support events like audits and/or discussion on the trend of the RIOs over time.

For administrative/security purposes, the tool should also support the assignment of user permissions. This capability allows the tool administrator(s) to grant the appropriate controls for users, ensuring that users only have the ability to access the data they require. This feature aids in CM control of the RIOs, while allowing a larger number of users access to the data contained within the tool.

Roles and Responsibilities

Table 6-1, below, defines the functions of the major participants in the RIO management process.

Title	Responsibilities
Organization Manager	• Establish and implement the organization's RIO Management Policy • Coordinate alignment of the organization's RIO Management Policy with the FAA Acquisition Management System (AMS) and the FAA Systems Engineering Manual (SEM) • Implement the organization's RIO Management Plan • Establish their respective RIO Management team [including the makeup of their RIO Management Board (RMB)] and allocate resources needed to support the organization's RIO Management Plan • Assist with managing RIOs in their control in accordance to the organization's RIO Management Plan • Participate and chair their recurring RIO Management Board and RIO Review Meetings • Coordinate with their RIO Manager(s), and External Stakeholder senior leadership, when required
RIO Manager	• Support the Organization Manager in implementing the organization's RIO Management Plan • Assist individual team members with all aspects of executing the organization's RIO Management Plan • Ensure RIO status and metrics are reported • Facilitate the organization's RMB and other supporting meetings • Assist with managing RIOs in their control in accordance with the organization's RIO Management Plan • Assist with coordinating RIOs in their control with external stakeholders when required
RIO Owner	• Support the organization's RIO Management Plan • Develop and manage their respective RIOs in accordance with the organization's RIO Management Plan • Assess their respective RIOs, develop plans, and monitor results • Ensure their respective RIO status and metrics are reported to applicable program management • Participate in RIO Management Boards (RMBs) and other supporting meetings

RIO Plan Owner	• Support the organization's RIO Management Plan • Assist the RIO Owner in creating plan options and assist with the development of supporting steps • Manage their respective RIO plans in accordance with the organization's RIO Management Plan • Assess their respective plans and monitor results • Participate in RIO Management Boards (RMBs) and other supporting meetings
RIO Step Owner	• Support the organization's RIO Management Plan • Assist the RIO Owner in creating approach options and assist with the development of supporting steps • Manage their respective RIO steps in accordance with the organization's RIO Management Plan • Assess their respective steps and monitor results • Participate in RIO Management Boards (RMBs) and other supporting meetings
Organization Team Member	• Identify new risks, issues, and opportunities • Assist in the analysis and assessment of RIOs based on their individual areas of expertise and experience • Contribute to the identification of plan approach(es) for identified RIOs and assist with the development of supporting steps. • Collaborate with the RIO Owner and program stakeholders to manage the RIO, within the scope of their areas of responsibility • Participate in RIO Management Boards (RMBs) and other supporting meetings

Table 6-1. RIO Team Roles and Responsibilities

DO: Perform Risk, Issue, and Opportunity Management

The RIO Management Process establishes the steps and flow required to perform RIO management. The process includes five steps that are repeated on an as-needed basis, as shown in Figure 6-2. These steps are:

1) Identify
2) Analyze & Assess
3) Develop RIO Plan
4) Execute RIO Plan, and
5) Track & Monitor

This section describes the assignment of specific responsibilities for the management of RIOs and prescribes the documenting, monitoring, and reporting processes to be followed. This process is designed to provide the:

- Framework for conducting RIO management
- Approach for identifying RIOs, including data sources and techniques to be used
- Method for performing qualitative assessments, including likelihood and impact
- Methods for reducing the overall likelihood and impact of RIOs, through the identification and implementation of tailored plans
- Method for tracking and reporting RIOs to the oversight organizations

Figure 6-2. Risk, Issue and Opportunity Management Process

Step 1: Identify

RIO Identification is defined as a systematic effort to uncover events or situations that may hinder (risk/issue) or improve (opportunity) achievement of program/portfolio objectives. RIO identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status. RIOs can be identified and defined by all team members based on the current environment and are submitted for initial review and information gathering. Once necessary information regarding the RIO has

been gathered, the RIO is presented for approval. If approval is not obtained due to a lack of sufficient information, further vetting will be conducted.

While potential RIOs may have many different root causes, the identification process isolates those conditions that may affect program technical performance, cost performance, or the program schedule.
Potential sources of RIOs include:

- Programmatic changes (including schedules and cost milestones)
- Unfavorable trends in Technical Performance Measures, predicted system performance, schedules, and financial status
- Design/program/peer reviews
- Proposal changes (including proposed changes in requirements)
- Unforeseen major events
- Newly identified RIOs
- Special assessments (at the direction of agency management)
- Changes or risks in interdependent programs
- Environment changes
- Use of commercial, off-the-shelf (COTS) solutions
- Safety and Security Risks

Figure 6-3 is the risk management risk identification flow for FAA projects and programs. The risk identification step is performed during each stage of the project or program or whenever significant changes occur in plans or project status. All stakeholders, users, suppliers, and execution teams participate in risk identification.

Special criteria are imposed on the risk identification process in order to accommodate **safety-** and **information-security-**related risks.

- Safety risks are not identified until a hazardous situation has been identified. The process starts with an analysis, which identifies potential hazards that are the basis for identifying safety-related risks. Chapter 31: System Safety Engineering contains more information on this topic.
- Information security risks are not identified until a combination of a viable threat coupled with vulnerability in the system that is capable of being exploited by the threat is discovered. Only then does the security community moves to declare a security risk. Chapter 30: Information Security Engineering contains more information on this topic.

During the RIO Identification step, it is important that a concise and accurate statement be written so that management and stakeholders clearly see the

source of the RIO. A properly worded RIO statement improves the ability to properly analyze the RIO, make accurate assessments, and to select appropriate RIO strategies.

Risk statements summarize the important attributes of a probable event and its associated risk and the impact that may occur if risk is not addressed. An example of a proper risk statement is provided in the following construct: “If, as a result of [condition present] an [uncertain event] occurs, then there may/could be [resulting situation with a negative impact].”

An issue statement is a statement of fact that captures clearly and concisely the important details of the situation, including dates and locations. A well-written issue statement includes the cause and the resulting negative outcome so that they can be analyzed to create the most effective plan. Although risk statements are written in an “if, then” format, an issue statement has no designated structure. The purpose of the issue statement is to enable managers, program team members, and stakeholders to understand the source and nature of the issue. Understanding the issue statement will improve one’s ability to analyze the issue properly, make a reasoned assessment of impact, and effectively communicate the issue information to those within and outside of the program.

An opportunity is described using an opportunity statement and the desired outcome. A well-written opportunity statement includes the conditions upon which the opportunity is dependent as well as the desired positive effects to be gained from realizing the opportunity. The opportunity statement enables stakeholders to understand the source and nature of the opportunity by clearly and concisely presenting important details, including dates and locations. It is preferred that opportunity statements are written in an “if, then” format. The critical conditions should be articulated in the opportunity statement so that it can be analyzed to create the most effective plan.

An example of an opportunity that can be identified is: If the logistics (e.g. equipment) are identified early enough in the project lifecycle. there can be savings to time and money as well as mitigating future risk in the blending of technologies into FAA systems.

At the conclusion of the identification step, there will be a list of potential RIOs that may affect project cost, schedule, and/or technical performance of the program. This list is validated to ensure that the RIOs identified are germane. The list also entered into the organization’s master RIO database and assigned a “RIO Owner”. The “RIO Owner” manages the efforts associated with the RIO from this point forward.

Step 2: Analyze and Assess

RIO Analysis is defined as an evaluation of the identified RIOs to determine possible outcomes, the likelihood of those events occurring, and the consequences of the outcomes. The likelihood and consequence are considered independently. They are mapped into an appropriate grid, also known as a Probability Impact Diagram (PID), to determine one quantitative figure of merit that represents the combined effects of likelihood and consequences called ”RIO exposure” or “Rating.” Assigning a RIO exposure to each RIO aids project management by prioritizing RIOs from most severe to least severe. This mapping also facilitates trend analyses of RIOs throughout their life cycle.

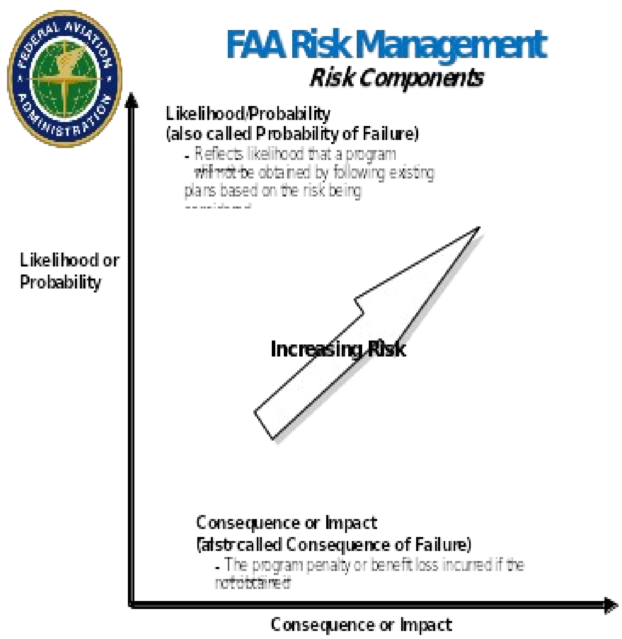


Figure 6-3. Risk Components

After the identification phase, an analysis and assessment of the RIO is conducted. All assumptions considered when analyzing the RIOs are documented. The rating (assessment) is reviewed and an approval determination is made. The “root cause” of the RIO should be stated so that the cause of the particular uncertainty is well understood and that program management has sufficient detail for analysis and assessment. In addition, analysis of RIOs may include more in-depth qualitative and/or quantitative analysis techniques.

RIOs are continuously re-analyzed and re-assessed. Re-analysis includes evaluating all components of the RIOs for updates, i.e. statement, rating, and plan. This evaluation includes identifying RIOs for RMB reassignment, considering RIO Status changes, as well as evaluating RIO to be transferred to an external stakeholder outside of the PMO. Similar to when a RIO is

initially assessed, approval of all proposed changes during the re-assessment is required.

Risk likelihood is the probability that a negative event will occur. The definitions found in Table 6-2, below, will be used as a guide in assessing likelihood.

Level	Likelihood	Description	Probability
A	Low: Not Likely	Existing approach and processes will effectively avoid or mitigate the risk, based on standard practices.	0% < Prob. <= 20%
B	Minor: Low Likelihood	Existing approach and processes may mitigate the risk, with minimal oversight based on similar cases.	20% < Prob. <= 40%
C	Moderate: Likely	Existing approach and processes may mitigate the risk, but alternative approach(es) may be required.	40%< Prob. <= 60%
D	Significant: Highly Likely	Existing approach and processes cannot mitigate the risk, but different approach(es) might.	60% < Prob. <= 80%
E	High: Near Certainty	Existing approach and processes cannot mitigate the risk; no known processes or alternatives are available.	80 % < Prob. < 100%

Table 6-2. Risk Likelihood

Risk Impact is a measure of the effect on program goals if the risk were to occur. The following definitions in Table 6-3 will be used as a guide for determining consequence. Note that the affected program baseline is an input to the process for determining the impact level.

Level	Impact	Technical	Schedule	Cost
1	Low: Program/ portfolio success not impacted.	Technical goals will still be met.	Schedule will still be met.	0% < Cost increases <= .1%
2	Minor: Negligible impact to program/ portfolio success.	Minor performance shortfall (within acceptable limits); no design or process change needed.	Schedule slip but able to meet key dates with additional activities or effort; critical path not affected.	.1% < Cost increases <= 1%
3	Moderate: Limited impact to program/ portfolio success.	Moderate performance shortfall; workarounds available, with minor design or process change needed.	Some key dates missed; workarounds available; critical path not affected.	1% < Cost increases <= 5%
4	Significant: Program/ portfolio success could be jeopardized.	Unacceptable performance; workarounds available, with significant design or process change needed.	Critical path affected; workarounds available; major milestones not affected.	5% < Cost increases <= 10%
5	High: Program success in doubt.	Unacceptable performance; workarounds not available.	Cannot achieve major milestones; rebaseline required.	Cost increases > 10%

Table 6-3. Risk Impact

The definitions shown in Table 6-3 (Risk Impact) will be used as a guide for determining issue impact. Note that the affected program baseline is an input to the process for determining the impact level.

The assessment performed below (impact) defines whether the issue is classified as low, medium, or high, issue level. This allows management to effectively assign resources to those issues that are deemed more significant to the overall success of the program.

Low Risk: Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Normal emphasis/effort, coordination, and normal monitoring will probably overcome difficulties.

Medium Risk: May potentially cause some increase in cost, disruption of schedule, or degradation of performance. Special emphasis, close coordination, and close monitoring will probably be able to overcome difficulties.

High Risk: Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Concerted and continual emphasis, coordination, and close monitoring will probably not be sufficient to overcome difficulties.

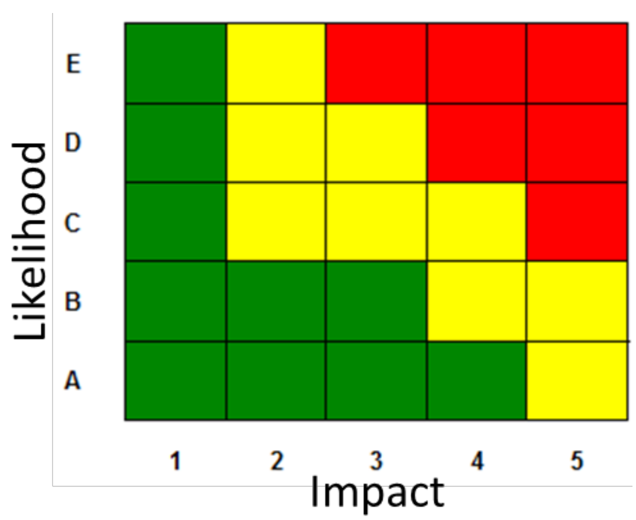


Figure 6-4. Risk Level Grid

An issue is an event or situation that has occurred or is certain to occur and its impact measures the effect on program goals.

The Likelihood of issues does not require assessment based on their probability of occurrence, 100%, so only Row E of the Risk Level Grid in Figure 6-4 is used to assess issue likelihood.

Low Issue: Little or no impact for increase in cost, disruption of schedule, or degradation of performance. Normal emphasis/effort, coordination, and normal monitoring will overcome difficulties.

Medium Issue: Some increase in cost, disruption of schedule, or degradation of performance. Special emphasis, close coordination, and close monitoring will be able to overcome difficulties.

High Issue: Significant increase in cost, disruption of schedule, or degradation of performance. Concerted and continual emphasis, coordination, and close monitoring will not be sufficient to overcome difficulties.

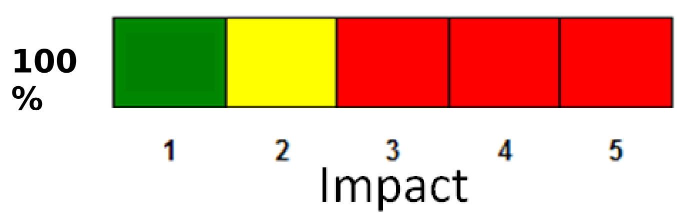


Figure 6-5. Issue Level Grid

Opportunity likelihood is the probability that a positive event will occur. The following definitions shown in Table 6-4 will be used as a guide in assessing likelihood.

Level	Likelihood	Description	Probability
A	Low: Not Likely	Unlikely to achieve the opportunity; no known processes or alternatives are available.	0% < Prob. <= 20%
B	Minor: Low Likelihood	Existing approach and processes cannot achieve the opportunity, but different approach(es) might.	20% < Prob. <= 40%
C	Moderate: Likely	Existing approach and processes may achieve the opportunity, but alternative approach(es) may be required.	40% < Prob. <= 60%
D	Significant: Highly Likely	Existing approach and processes may achieve the opportunity based on similar cases.	60% < Prob. <= 80%
E	High: Near Certainty	Expected to achieve the opportunity based on existing approach and processes.	80 % < Prob. <= 100%

Table 6-4. Opportunity Likelihood

Opportunity impact is the positive effect on program goals if the opportunity is achieved. The following definitions shown in Table 6-5 will be used as a guide for determining impact. Note that the affected program baseline is an input to the process for determining the impact level.

Current Baseline				
Level	**Impact**	**Technical**	**Schedule**	**Cost**
1	Low: Program/ portfolio not impacted.	Slight increase to claimed benefits.	Slight acceleration of schedule, but key dates not impacted; critical path not affected.	0% < Cost savings <= .1%
2	Minor: Negligible impact to program/ portfolio.	Some increase to claimed benefits.	Some acceleration of tasks, but key dates not impacted; critical path not affected.	.1% < Cost savings <= 1%
3	Moderate: Moderate impact to program/ portfolio.	Moderate increase to claimed benefits.	Acceleration of some key dates; critical path moderately improved.	1% < Cost savings <= 5%
4	Significant: Major impact to program/ portfolio.	Major increase to claimed benefits.	Major acceleration of schedule; critical path optimized.	5% < Cost savings <= 10%
5	High: Significant impact to program/ portfolio.	Significant increase to claimed benefits.	Significant acceleration of milestones; rebaseline required.	Cost savings >10%

Table 6-5. Opportunity Impact

The Opportunity Level Grid in Figure 6-5, below, follows the same basic pattern as the Risk Level Grid in Figure 6-4, above. The ranking of the cells in

the grid allows management to effectively assign resources to those opportunities that are deemed more significant to the overall success of the program.

Low Opportunity: Minor increase in benefits to the program/organization with minimal schedule acceleration and cost savings. Or minor expansion of program/organization benefits with significant schedule duration and costs incurred. Concerted and continual emphasis, coordination, and close monitoring will probably not be sufficient to achieve the opportunity.

Medium Opportunity: Some increase in benefits to the program/organization with moderate schedule acceleration and cost savings. Or some expansion of program/organization benefits with moderate schedule duration and costs incurred. Special emphasis, close coordination, and close monitoring will probably be able to achieve the opportunity.

High Opportunity: Significant increase in benefits to the program/organization with maximum schedule acceleration and cost savings. Or significant expansion of program/organization benefits with negligible schedule duration and costs incurred. Normal emphasis/effort, coordination, and normal monitoring will probably achieve the opportunity.

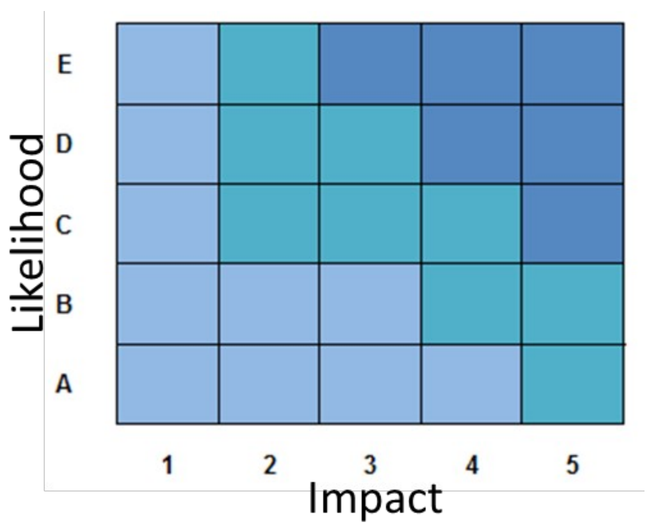


Figure 6-5. Opportunity Level Grid

Step 3: Develop RIO Plan

The objective of RIO plans is to address the scope of the RIO. RIO plans consist of a specific course of action, approach concept(s), and discrete steps for each applicable RIO, and must be for all RIOs with an approach strategy of Control.

- For risks, the objective of the plan is to reduce the likelihood of occurrence and/or negative impact if the risk is realized.
- For issues, the objective of the plan is to reduce the issue's negative impact
- For opportunities, the plan outlines the steps to improve the likelihood and/or positive impact.

A contingency plan description can be developed if there is concern about the success of the first-choice plan When it is determined that the first-choice plan is not achieving the desired results, the RIO will be reassessed & analyzed in accordance with the contingency plan description.

The RIO Management process provides the framework for developing plans to take action, or deliberate decisions to take no action, in order to address program RIOs. The plan strategy options are defined in Table 7 below. For all identified RIOs, the various strategies should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, the effect on the system's technical performance, and the most suitable strategy selected. The most commonly utilized strategy option for managing RIOs is Control.

Plan Strategy	Definition
Avoidance	Avert the potential of occurrence and/or impact by selecting a different approach than planned.
Transfer	Shift the RIO to another organization.
Control	Develop options and alternatives for taking action to address the RIO.
Assumption	Accept the likelihood/probability and the impacts associated with a RIO's occurrence.
Research and Knowledge	Expand experience and subject matter expertise

Table 6-6. Plan Strategy Definitions

Once a plan strategy has been chosen, a high-level plan description is generated. This description can include the use of multiple methods (approaches) for addressing the RIO. Individual plan steps are defined to support the methods.

Plans consist of a series of steps that when completed reduce the rating of the RIO to an acceptable threshold for the program. When developing the plan steps, interdependences should be identified and considered, when applicable. This level of detail will enable the organization to monitor the progress of reducing the likelihood and impact of risks and issues and achieving desired opportunities. Also, it is possible to develop multiple plan approaches simultaneously in order to determine the best plan.

There are several times during a program/project's life cycle that provides an appropriate "decision point" that may trigger a re-assessment of RIOs. Examples of those decision points include, but are not limited to:

- New phase or stakeholder
- Key program milestone approaching
- Time since last assessment

Step 4: Execute RIO Plan

Once the organization decides on a RIO Plan, the decision is implemented and carried out effectively so that RIO likelihood, consequence, or both, are reduced to an acceptable level. RIO reduction implementation requires that the associated specific tasks be incorporated into the planning, scheduling, budgeting, and cost-accounting systems used by the program.Mitigation activities are shared with and communicated to all stakeholders.

Step 5: Track and Monitor

Existing RIOs are tracked and monitored periodically, on an event driven basis, or continuously. This includes obtaining RIO updates, including individual step updates. Tracking and monitoring enables the development of metrics to provide meaningful information to management, to enable informed decision making, and optimize the management of their programs.

CHECK: Monitor and Track Risks

This Phase of the RIO PDCA cycle is dedicated to monitoring and tracking risks throughout the lifecycle.

ACT: Update as needed

Process improvement involves correcting deficiencies identified in the Check phase of the PDCA cycle. Updates to RIO Management Plans and Implementation Strategies should be made to reflect changes in approach, schedules, resources and other impacts as necessary.

***Special Considerations for System of Systems**
As systems are combined into a system of systems (SoS), the tasks of RIO management increase in difficulty. Although the area of SoS RIO Management is young, with little applicable research, some of the challenges and guidance are presented. As research and case studies are published, better techniques will undoubtedly be discovered for handling an SoS.

In an SoS, the constituent systems operate autonomously with their own program manager and systems engineers. Many systems may be in operation while others are in development. However, the nature of the SoS means a RIO to any one system may have its source in another system. And there is no guarantee that the source system is affected by the RIO. The systems engineer needs to watch for RIOs in all of these systems, operational and developmental. The problem is that any system external to one's own is outside of any direct control. Of course the systems engineer must always worry about external RIOs, but these RIOs may ripple through the SoS or only emerge as part of the SoS.

The RIO process described in PDCA cycle "Do" directly applies to SoS RIOs. When implementing each step of the process consideration has to be given to the added complexity of working between multiple programs. An example of this may be the need to establish a management structure to appropriately control the RIO throughout its lifecycle.

***Special Consideration for Commercial, Off-the-Shelf Systems**
Selecting a COTS-based acquisition has implications to RIO Management. COTS has an inherent set of concerns that are usually driven by the market. These concerns need to be addressed through the use of the RIO management process. Refer to FAA COTS Risk Mitigation Guide for more information.

Outputs

The primary outputs of the RIO Management PDCA Process are:
- RIO Management Plan
- Implementation Strategy
- RIO Register
- RIO Database
- RIO Metrics
- RIO Mitigation Plan Summary
- RIO Summary

- RIO Mitigation Plans

It is recommended that the Risk Summary, Risk Mitigation Plan Summary, and the Risk Status be communicated regularly to all stakeholders. Management decisions are made as a result of the abovementioned outputs, therefore it is important that they be properly maintained throughout project effort.

Interdependencies

Special Considerations for System of Systems
System Safety
Information Security

FAA Sources for More Detailed Information

FAA RIO Scorecards
FAA COTS Risk Mitigation Guide

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

7 – Configuration Management Process

Introduction

Configuration Management (CM) provides a structured approach to identify, control, and maintain the configuration of a system during its life cycle. The CM process establishes and upholds the consistency of a system's performance and its functional and physical attributes with its requirements, design, and operational information throughout the life cycle. Configuration Management guarantees that system performance and functional/physical attributes are properly identified, documented, validated, and verified to preserve integrity. Additionally, CM ensures that any changes to these system attributes are identified, reviewed, approved, documented, and implemented.

Imperative to Configuration Management is the establishment of baselines. A **baseline** is an agreed-to description of the attributes of a product at a point in time that serves as a basis for defining change. Establishing the system baselines, along with the control and maintenance of these baselines make managing a system moving through the life cycle much easier. Controlling changes to these baselines is the other aspect of CM. The FAA **Configuration Control Board (CCB)** authorizes the establishment of configuration baselines and the review and actual changes to these baselines. A CCB ensures the functional and operational integrity of a baseline through establishment and enforcement of effective change management and control practices and processes. The NAS CCB is the highest ranking CCB in FAA and it is established by the FAA Administrator. The NAS CCB has authority to charter subordinate CCBs as necessary. The service units typically develop their own CCB charter and operating procedures upon assignment of a NAS program or programs. Configuration Management keeps the inevitable changing of project artifacts under control by eliminating the confusion, and errors that result, from dealing with multiple versions of project artifacts as well as the issue of unauthorized changes to these artifacts.

Configuration Management occurs during the "Do" phase of the PDCA cycle (Plan, Do, Check, Act) for the Technical Management processes. It is an iterative process in that it provides a closed-loop process for managing change. Configuration Management begins at the project's inception and is applied throughout the entire life cycle.

The Configuration Management PDCA cycle is depicted in Figure 7-1. The major outputs of the CM process are the established baselines, updated baselines, baseline change documents, and configuration status reports.

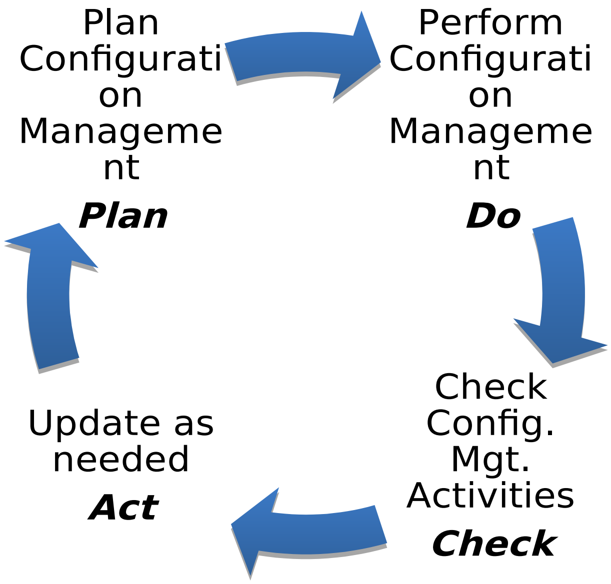


Figure 7-1. Configuration Management PDCA Cycle

Objective

The Configuration Management Process establishes and maintains the integrity of all identified outputs of a project or process and makes them available to all concerned parties.

Inputs

An input to the Configuration Management Process is information that the CM process needs that provides directions; is the basis for or otherwise drives CM process activities; or requires action through one or more CM tasks.

The primary inputs to the CM process are described below:

FAA Policy

- **FAA Order 1800.66 "National Airspace System Configuration Management Policy"**. FAA Order 1800.66, prescribes the requirements and details of the processes and procedures to perform CM of the NAS. The introduction of new products and services to the NAS or any changes to existing products or services must be

accomplished in accordance with FAA Order 1800.66. This policy is a standalone document and is part of the FAA Acquisition Management System (AMS).

Change Requests

- **External Change Requests** are used by outside parties to request changes to FAA-managed baselines.
  - **Engineering Change Proposals (ECP).** ECP manages allocated and product baselines, as well as any subsequent changes to these documents. ECPs are used by the contractor.
  - **Requests for Deviations and Waivers –** During product development or production, there may be instances in which deviations or waivers to requirements are needed. The contractor then submits a request to deviate from (planned) or waive (unplanned) a specific requirement, as applicable. The contractor submits requests for deviation (RFD) or requests for waiver (RFW) to FAA. RFDs/RFWs are generally temporary and are brought into compliance at a later time.
  - **Contractor Change Vehicles –** The contractor's/developer's approved CM plan documents other contractor change vehicles that affect the change process.
  - **Memoranda of Understanding (MOU) –** MOU is a documented agreement between FAA organizations or between FAA and an external organization when no formal contractual relationship exists between the parties. MOUs serve as source data to be kept as part of the program documentation and used to drive, validate, and verify program activity as necessary during the CM process.
- **Internal Change Requests** are used when changes are requested to CIs by parties within FAA. FAA uses NAS Change Proposals to accomplish this.
  - **NAS Change Proposal (NCP)** – The NCP is the coordination vehicle used internally to formally change NAS baseline documentation.

Systems Engineering Management Plan (SEMP)

- **Configuration Management Plan**. Configuration Management Plan describes the CM strategy, implementation activities, and standard practices for performing CM for the project of interest.
- **Work Breakdown Structure (WBS)**. The WBS provides a logical structure for developing the products that will be placed under CM. This structure assists CM in establishing the Configuration Items.

Configuration Definitions

Configuration Definitions provides definitions and supporting information for those items under CM.
Some examples are:

- **Facility Definitions**
- **Product Definitions**
- **Decision Analysis Reports (DARs)**

Configuration Documents

Configuration Documents are any documents given to CM for retention.
Some examples are:

- NAS Enterprise Architecture.
- Requirements (NAS-RD, PRD, SSD, IRD, ICD)
- Validated Tools and Reference Models
- Test article configuration
- Test apparatus configuration

Change Release Notes

Change release notes provide documentation of change completion when a change is requested. It specifies what has been changed, approval authority, and installation or implementation date. Change release notice information is a key component of configuration status accounting.

Configuration Status Accounting Reports (CSAR) Updates

CSAR updates provide the current status of MCI configuration items or work products from Lifecycle Engineering to keep CM status current.

Configuration Management Process Elements

PLAN: Plan Configuration Management

Planning for configuration management is key to successfully reaching project goals. Planning provides the basis for ensuring application of effective and efficient CM practices throughout each of the applicable SE processes.

Configuration Management Planning activities are:

1. Develop a Configuration Management Plan

Step 1: Develop a Configuration Management Plan

CM planning determines the resources for the CM activities throughout the lifecycle, establishes the mechanisms for performing the CM process,

designates the responsibilities of the organizations performing the CM process, and ensures that control will be extended to vendors and contractors during the equipment acquisition. The Configuration Management Plan will address all of these issues. The CM plan ensures that the integrity and continuity of the design, engineering, and cost tradeoff decisions made among technical performance, producibility, operability, testability, and supportability are recorded, communicated, and controlled by program and functional managers. The Configuration Management Plan can be found in the SEMP for the project of interest, however, there may be instances where it is a standalone document. CM planning enables the process activities completed during the "DO" phase of the CM PDCA cycle.

At a minimum, a good Configuration Management Plan should address the following:

- Identify Stakeholders
- Identify and Gather CM process inputs
- Identify CM tool, when applicable
- Establish schedule for CM activities
- Establish Communication Plan with Stakeholders
- Establish a Configuration Control Board (CCB)
    - A **CCB** is the FAA authorized forum for establishing configuration management baselines and for reviewing and acting upon changes to these baselines. A CCB ensures the functional and operational integrity of a baseline through establishment and enforcement of effective change management and control practices and processes. Each CCB develops operating procedures according to its specific mission and needs. FAA Order 1800.66 provides requirements for developing and maintaining CCB charters and operating procedures.
- Establish CM Procurement Requirements
- Establish CM Procurement Strategy

DO: Perform Configuration Management

Configuration Management is performed according to the Configuration Management Plan developed during the "Plan" phase of the CM PDCA cycle. Each process activity must be applied appropriately to maximize the benefits that can be obtained through Configuration Management. Each supporting activity can also be tailored to meet the mission and needs of the project of interest. These tasks are iterative and can be completed as often as needed.

The Configuration Management Process activities are:

1. Identify Configuration
2. Select Configuration Items
3. Establish and Maintain Baseline
4. Manage Approved Baseline Changes
5. Provide Configuration Status Accounting
6. Verify and Audit Configuration

Each is described below.

Step 1: Identify Configuration
Configuration Identification is the systematic process of selecting product attributes, organizing associated information about the attributes, and stating those attributes. It includes assigning and applying unique identifiers for the product and its associated documentation, as well as maintaining document revision relationships to the product configurations. Product attributes are applied to hardware, software, firmware, and their associated documentation. These attributes mature through each of the lifecycle phases and, at key milestones during those phases, are validated and incorporated into the baseline.

Step 2: Select Configuration Items (CI)
A **Configuration Item (CI)** is an aggregation of hardware, software, processed materials, services, or any of its discrete parts that is demonstrated for CM and treated as a single entity into the CM process. Selecting CIs separates the elements of a system or product into individual subsets to manage their development and subsequent change. The process steps for selecting CIs in the FAA are as follows:

- Establish program and program identification
- Plan acquisition strategy
- Select Configuration items
- Update

Refer to FAA Order 1800.66 for more information on selecting CIs.

Step 3: Establish and Maintain Baseline
The progression of a product through its lifecycle appears as a series of baselines. Key product milestones provide a snapshot of the product configuration at the respective lifecycle phase. Baselines are established by agreeing to and recording the stated definition of a CI's attributes. They typically include specific revision or version of approved and released documents, sets of documents, or electronic files (software or information)

that serve as the basis for managing change. Because of the complexity of the NAS, FAA maintains an enterprise-level baseline and several other baselines that are established for an acquisition program. There are five baselines, each described below: Functional, Allocated, Product, Facility, and Operational.

Functional Baseline – The functional baseline is the approved documentation describing the system's functional, performance, interoperability, and interface requirements and the verifications required to demonstrate achievement of those specified requirements. The functional baseline represents the functional requirements for a program and is the first formal program baseline to be established after concept exploration. FAA has the NAS functional baseline, which is made up of the NAS-level requirements, and the final program requirements.

Allocated Baseline – The allocated baseline is the approved documentation describing a CI's functional, performance, interoperability, and interface requirements that are allocated from the requirements of a system- or higher-level configuration item; interface requirements with interfacing configuration items; and the verifications required to confirm the achievement of those specified requirements. The allocated baseline represents the program's design requirements. This baseline is typically established just before contract award after the system requirements review. The allocated baseline for FAA is the System Level Specification and Interface documentation that will be used for an acquisition program.

Product Baseline – The product baseline is the configuration of the system or product being delivered to the customer. It consists of the combined performance/design documentation used in Configuration Identification for production/procurement. This documentation package incorporates the allocated baseline documents describing a Configuration Item's (CI's) functional, performance, interoperability, and interface requirements and the verifications required to confirm achievement of those specified requirements. It also includes additional design documentation, ranging from form and fit information about the proven design to a complete design disclosure package, as deemed necessary for CI acquisition.

Facility Baseline – The facility baseline is the information needed to identify and control changes as well as record configuration and change implementation status of all CIs under Regional CCB authority. There are two important categories of facility data subject to CM: facility baseline drawings and engineering data such as critical power panel schedules. This baseline is an essential element of FAA planning for introducing NAS

systems/subsystems. Establishment of a facility baseline is determined by assessing the impact of Capital Investment Plan projects as well as regionally and nationally initiated changes and improvements.

Operational Baseline – The operational baseline is the approved technical documentation representing installed operational hardware and software. This represents a product baseline adapted to local conditions. Operational baselines comprise the technical documentation that initially describes a delivered system. They also include changes to that delivered system that occur as a result of in-service modifications/improvements or as a result of the addition of FAA-developed documentation/tools. The operational baseline includes the product baseline and any subsequent changes to it. Operational baselines describe the system as deployed in the NAS.

Step 4: Manage Approved Baseline Changes

Baseline changes are managed through Configuration Control. **Configuration Control** is the systematic process that ensures that baseline changes are properly identified, documented, evaluated, and approved by the appropriate level of authority and implemented and verified. Baseline changes may be triggered by a modification of the product, product information, or associated interfacing products. The following steps must be completed in order to implement changes to approved baselines.

Step 4.1 Identify and Describe Change

Changes to Baselines are documented on the applicable change vehicles. In the FAA, any person can identify a problem or suggest an improvement at any time during the product lifecycle. The factors determining the type of change vehicle or the need for a change vehicle are the type of baseline, who is responsible for controlling the baseline, and the CM plan. Change vehicles state the problem or need for change, the proposed change, affected CI, cost, and scheduled for change implementation, and so forth. Change vehicles are uniquely identified and require the baseline elements affected.

Step 4.2 Evaluate Change

Coordination and review of changes embody the systematic approach for ensuring the validity, feasibility, and assessment of impacts of the change. Formal reviews capture each reviewer's name, organization, comments, date of review, and appropriate resolution of comments as applicable. Reviews must occur before adjudication. This approach includes reviewing changes to both formal and informal baselines.

Step 4.3 Ensure Disposition of Change

Change disposition is the conclusion by the appropriate authority that the item submitted for approval is either suitable or unsuitable for implementation or release. CCBs serve as the forum for adjudicating

changes or formal baselines. Each CCB is an independent decision-making body within its prescribed level of authority. A CCB has decision authority for all changes affecting CIs assigned to the CCB. These CCBs may approve any change as long as the CI is assigned to that CCB.

Step 4.4 Monitor Change Implementation

An important CM function is monitoring change implementation. This ensures completion and release of approved changes. Change implementation is accomplished by closure of Configuration Control Decision (CCD). The **Configuration Control Decision (CCD)** is the official FAA notification of CCB decisions and directives. The CCD identifies required actions and the organizations responsible for completing either implementation of approved changes or follow-up for disapproved changes. CCD actions may include:

- Approval of physical incorporations of changes to affected hardware, software, or facilities
- Approval of technical evaluations, studies, or tests
- Directions for incorporation of changes in baseline documentation.
- Field modification installation and tracking when changes are needed to facilities or operational equipment

Step 5: Provide Configuration Status Accounting (CSA)

Configuration Status Accounting (CSA) is the systematic recording and reporting of system or product configuration status. CSA includes baseline change status and history for all items shown in the MCI, from initial delivery to the end of product service. CSA reports not only communicate status, but also support conduct of formal configuration audits when design documentation is not available or has not been updated to the current configuration. CSA is performed at all levels of CM across the life cycle. The following is required to provide CSA.

Step 5.1 Capture Change Data

Capturing change data, typically by using the automated CM tool that was identified in the CM plan, enables recording and reporting of the status and history of baseline changes from initiation through implementation.

Step 5.2 Establish Baseline Configuration Status

Once any of the baseline types is established, it can exist in two states: baseline and baseline with changes outstanding. When the outstanding changes are incorporated into the affected baseline, they become the updated baseline. Updated baselines are established by integrating all the approved baseline changes and the updated baselines become the new baseline when approved.

Step 6: Verify and Audit Configuration
Conducting audits and quality checks ensures the integrity of the product. Functional and Physical Configuration Audits are examples of formal audit activities used to establish the product baseline. A functional configuration audit is intended to verify that the development of a CI has been completed and has achieved the performance and functional characteristics specified in the functional baseline and a physical configuration audit is a technical review of the CI to verify the "as-built" matches the technical documentation. Quality checks, peer reviews, or internal audits of work products are informal means for documenting and managing the quality and validity of informal organizational baselines

CHECK: Check Configuration Management Activities

Formal and informal reviews of the Configuration Management activities are required to ensure accuracy and completeness of the CM process.

Configuration Management Process checklist to consider:

- ✓ Have Configuration Management process activities been performed according to the Configuration Management Plan for the project of interest?
- ✓ Have Configuration Management activities been performed correctly and completely?
- ✓ Have all baseline changes been communicated to the appropriate stakeholders?
- ✓ Have all associated work products been updated to reflect baseline changes?
- ✓ Are inputs still relevant and valid?

ACT: Update as needed

This step of the Configuration Management PDCA cycle is reserved for making any updates to the CM process activities and associated work products. These changes can include updating the CM plan to reflect schedule, budget or organizational changes, revising the CM input list to reflect document name changes or updates, or repeating the CM process activities, if performed incorrectly previously. The specific updates will be directly related to the results of the "CHECK" phase of the Configuration Management PDCA cycle.

Outputs

The primary outputs of the Configuration Management process are:

- **Baselines and Updated Baselines** – Baselines are established during the CM process and any changes to these baselines are released in the form of updated baselines.
- **Baseline Changes** – Baseline changes are provided to all CM users whenever a potential change or update is pending that could impact their work product.
- **Configuration Status Accounting Reports (CSAR)** – Configuration status accounting reports (CSAR) provide the current status of CI configuration items or work products. CSARs can be generated electronically and provided on demand or at scheduled intervals by the supporting CM process.

Interdependencies

Integrated Technical Planning

External Sources for More Detailed Information

FAA Order 1800.66 “National Airspace System Configuration Management Policy”
EIA 649 “National Consensus Standard for Configuration Management”

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems engineering: System life cycle processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

This page intentionally left blank.

8 - Information Management Process

Introduction

The Information Management process collects, manages, stores, and distributes all information pertaining to a particular project. It applies various policies, procedures, and information technology to maintain the integrity of all information generated during a project's life cycle. The information management process ensures that the correct information is available when needed without compromising the information's security or value.

Information is any and all processed data and data is defined as raw, unorganized facts. Information exists in many forms and varies project to project. During the life cycle, much information is used, generated, and collected. The value of this information will depend greatly on its users. As projects and systems become more complex, so will their information and data. It will be critical to have a systematic way to keep all the information and data organized and managed throughout the life cycle. For the purpose of this manual, information and data will be used interchangeably.

Information Management occurs during the "Do" phase of the PDCA cycle (Plan, Do, Check, Act) for the Technical Management processes. Information Management is an iterative process and applies to all projects, regardless of size or complexity.

The Information Management PDCA cycle is depicted in Figure 8-1. The Information Management process provides accurate and secure project information in a timely manner that can be used as both inputs and outputs of the other systems engineering processes.

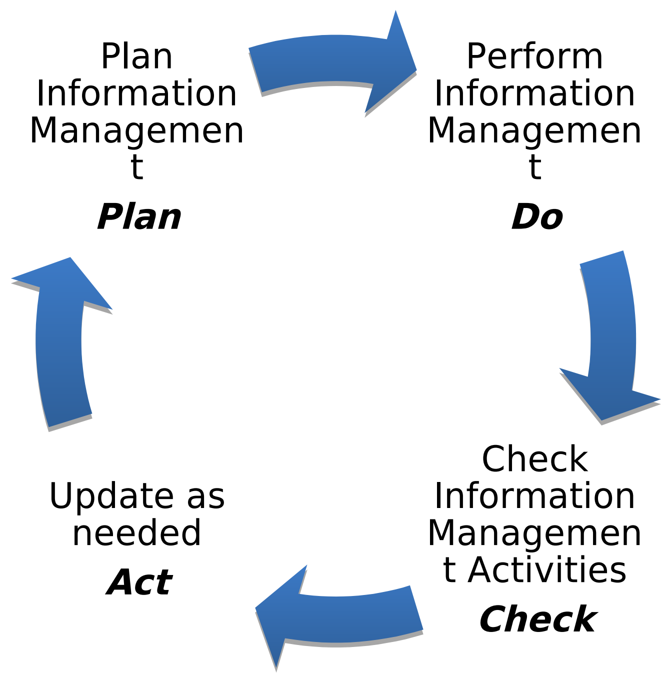


Figure 8-1. Information Management PDCA cycle

Objective

The Information Management process generates, acquires, approves, protects, archives, and distributes all project information to establish and maintain the integrity of the project.

Inputs

An input to the Information Management Process is information that the Information Management process needs that provides directions; is the basis for or otherwise drives information management process activities; or requires action through one or more Information management tasks.

The primary inputs to the Information Management process fall into 3 categories: Information Guidance, Information Products, and Information Requests. Each is described below.

Information Management Guidance. Information Management Guidance refers to any and all documentation with which the Information Management PDCA cycle activities must comply. They include any and all information that provides any stipulations, restrictions, or instructions on how project information is to be acquired, maintained, or stored. Some Information

Management Guidance may even address who can and cannot gain access to certain project information. Some examples of Information Management Guidance include:

- FAA policy, procedures, and orders
- Standards
- Program policy and procedures
- FAA and organizational agreements
- FAA legislation

Information Products. Information products refer to any and all information that the Information Management process will manage. The information products will depend on the scope of the project and will vary from project to project. The project manager and systems engineer will work together to determine a project's information needs. Information products can be any recorded information, regardless of the form or method of recording. This can include administrative, managerial, financial, and technical data. The information products will evolve as they move through the life cycle and it will be imperative to successfully implement the information management process, to ensure that the information products remain current and up to date. Information products are the primary input to the Information Management process. Some examples of information products include:

- Concept of Operations (CONOPS)
- SEMPs, which include the project's Integrated Technical Plans
- NAS Enterprise Architecture information and Views, including the AVs, OVs, SVs, and TVs
- Contract Statement of Work
- Work Breakdown Structures
- Meeting Minutes
- Travel Receipts

Information Requests. Information requests are simply requests for information. Distributing project information and data is part of the Information Management process and information will mostly be distributed upon request. Information requests can come from a variety of sources and the fulfillment of these requests will be at the judgment of the project manager, primarily. Keeping a thorough record of information requests will help maintain the integrity of a project's information.

Information Management Process Elements

PLAN: Plan Information Management

Information Management provides the foundation for the acquisition, management, storage, and distribution of project information throughout the life cycle; therefore, adequate planning is necessary.

Information Management Planning Activities:

1. Develop an Information Management Plan

Step 1: Develop an Information Management Plan

The Information Management plan outlines how information will be acquired, managed, distributed, and stored. This plan is part of the project SEMP. The Information Management Plan should be tailored accordingly to fit the information needs for that project of interest.

At a minimum, a good Information Management Plan should address the following:

- Identify valid sources of information
- Identify valid list of project stakeholders
- Define information format requirements
- Define information storage requirements
- Define information access privileges
- Define information security requirements
- Allocate schedule for acquiring, maintaining, distributing, and retiring project information

DO: Perform Information Management

Using the Information Management Plan, Information Management is performed. All of Information Management process activities are conducted in compliance with the Information Management guidance available for that particular project. A project's information products are both inputs and outputs of this phase.

The Information Management Process activities are as follows:

- Acquire Information Products
- Maintain Information Products
- Distribute Information Products
- Archive Information Products
- Retire Information Products, when applicable

Each activity is described below:

Step 1: Acquire Information Products
Gathering the information that will be managed is the first step in performing Information Management. What information will be acquired, when information will be acquired, and how the information will be acquired varies from project to project, and is documented in the Information Management Plan. A project's Information Management strategy identifies a list of information sources, formats, security requirements, relevant guidance, and stakeholders. This ensures that credible, correct, and useful information is gathered on time without jeopardizing the information's integrity or violating any organizational, agency, or congressional policies, orders, or laws.

When the information is acquired, it becomes an information product. As stated earlier, an information product is recorded data of any nature, regardless of medium or characteristics. Most information products will be acquired electronically, although there may be some instances where information may need to be manually acquired.

Step 2: Maintain Information Products
After acquiring the information products, the next step is to maintain them as the project moves through the life cycle. What exactly it means to maintain the information products and what is required to do so will vary from project to project. Information maintenance will depend greatly on the type of information product and the information needs of the identified stakeholders. Some information will require more maintenance than others. The project manager and systems engineer will work together to determine how a project's information will be maintained as well as how often maintenance will be required. All of this information will be detailed in the project's Information Management plan.

Some common tasks in maintaining project information include:

- Storing information products for easy and expedited retrieval
- Prioritizing and reviewing information products to ensure, at a minimum, that they are accurate, relevant, valid, and complete
- Protecting information products from security threats and privacy breaches
- Protecting information products against hazards or natural disasters (*i.e.* fire, flood, earthquakes)

Step 3: Distribute Information Products
One of the major goals of Information Management is to make sure that information is available when it is needed. Having a formal process to manage a project's information allows for information to be distributed more easily and quickly.

Generally, project information will be distributed upon request and as needed. This will help maintain the integrity and security of the information products. Each request will be reviewed and evaluated to determine the requested information availability and the information privileges of the requester. Not all information requests will be granted. The access rights of the requester as well as information sensitivity, security, and availability are just a few of the reasons that can cause an information request to be denied.

The Information Management plan will detail how and when information products will be distributed for approved information requests for the project and ensure compliance with the necessary Information Management guidance. Proper maintenance of the information products will guarantee that the requested information is readily available in its proper format.

Step 4: Archive Information Products

During the life cycle, many information products are generated and some will need long-term storage, therefore becoming archived information products. Keeping a record of past information products will be useful in identifying lessons learned and best practices. Additionally, having historical data available will be a valuable resource in identifying project risks.

Which information products are archived will be at the discretion of the project manager and systems engineer. A project's Information Management plan will outline the archival requirements of the information products and the schedule for when they are archived.

Properly protecting and preserving archived information products will also be very important to this step. A majority of the archived information products will be unique and so it will be necessary to keep the information in a safe place.

Step 5: Retire Information Products when applicable

As a project moves through the life cycle, some information products will no longer be relevant, accurate, necessary or valid and will need to be discarded. This step will be completed on an ad hoc basis as the need to retire a project's information products arise. The project manager, along with the systems engineer, will work together to determine which information products are retired.

Even though the retiring information is no longer needed, there are still security and privacy issues that need to be addressed. Information products must be discarded in compliance with the project's available Information

Management guidance, security, and privacy requirements. Improperly disposing of information products could threaten the integrity of the other information products not being retired.

After performing Information Management, information products will be in a centralized location, protected, regularly maintained, available when needed, and retired when deemed no longer relevant.

CHECK: Check Information Management Activities

The information management process manages project information throughout the life cycle. Information Management activities will help preserve the integrity of the information products.

Information Management checklist to consider:

- ✓ Date and availability of Information Management guidance. Checking to make sure all the information activities are conducted according to most recent version of organizational policies, laws, and orders will ensure the information products’ integrity.
- ✓ Validity of information sources. Acquiring information products from valid sources will save money and reduce the information products accessibility to security threats and privacy breeches
- ✓ Access rights and privileges of information requesters. Ensuring that the correct people have access to the correct information will prove beneficial in the areas of information accuracy, security, and validity
- ✓ Information products storage locations. Storing information products in safe and secure locations benefits the entire Information Management process.

ACT: Update as needed

Checking the Information Management process activities may result in the need for change; those changes are made during this phase. These changes can include updating the information source list or the updates to the information products in general. Keeping track of the changes and informing all relevant stakeholders of those changes are imperative. The Information Management plan must also be updated to reflect those changes.

Outputs

The primary outputs of the information management process are timely, secure, correct project data and information.

Interdependencies

Integrated Technical Planning

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

9 – Technical Assessment Process

Introduction

The Technical Assessment process ensures that a project performs according to project plans, schedules, and within projected budget while meeting the technical objectives and expectations of the stakeholder. Technical Assessment measures and manages the technical progress of a project. Variances, potential risks, and any trends are a few examples of the types of information generated during the Technical Assessment process. The Technical Assessment process is a risk-reduction approach and promotes continuous communication between the systems engineers, project managers, and any and all relevant stakeholders.

The Technical Assessment process essentially monitors and controls the technical progress of a project. Within FAA, techniques are used to monitor technical progress of a project and the control aspect of the process is accomplished through the use of mechanisms. An example of a technique is the measurement of certain technical characteristics of the system compared against a predetermined baseline or set of standards. A mechanism is a control gate that assesses the progress of the system against criteria established for a given point in the system's life cycle. These gates typically take the form of technical reviews and audits. Technical monitoring and controlling are detailed more in the "DO" phase of the Technical Assessment PDCA cycle (Plan, Do, Check, Act).

Technical Assessment occurs during the "CHECK" phase of the PDCA cycle for the Technical Management processes. This process is used to check that the project of interest progressed through the life cycle as planned in the project Systems Engineering Management Plan (SEMP). The SEMP contains the Integrated Technical Plans. For more information on a SEMP, refer to Chapter 3: Integrated Technical Planning.

The Technical Assessment PDCA cycle is depicted in Figure 9-1. It is an iterative process and applies to all projects regardless of size and complexity. Technical Assessments occur at strategic point in the life cycle, but can occur more frequently if needed. The primary outputs of the Technical Assessment process are the results of the various assessments and reviews.

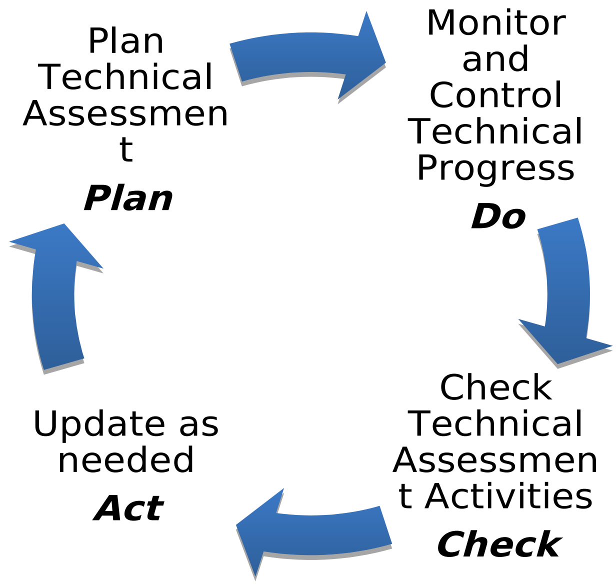


Figure 9-1. Technical Assessment PDCA cycle

Objective

The Technical Assessment process measures technical progress and the effectiveness of project plans and requirements.

Inputs

The primary inputs to the Technical Assessment process are:

- SEMP
- FAA Policy
- Standards
- Corporate Mission and Goals

Each is described below.

SEMP

The project SEMP establishes how the technical assessments and reviews are accomplished and what technical measures are used. Project measures are those technical characteristics of the project that will be tracked and compared against a predetermined baseline or set of standards. There are two types of project measures: **Technical** and **Project Performance**.

Technical Performance Parameters (TPP)

TPPs are the critical technical performance requirements that support critical operational needs and essentially measure the extent of success or failure of a design to meet those needs. The critical requirements are either selected or derived from Measures of Effectiveness (MOE). MOEs are the "operational" measures that are closely related to the achievement of operational objectives of the project. It must be possible to project the evolution (or maturation) of TPPs over time toward the desired value at completion of development. TPPs are directly linked to the critical requirements; so, it is very important to maintain that linkage as the requirements are changed, to fit the evolving needs of the project.

Project Performance Parameters (PPP)

PPPs are the nontechnical equivalent to TPPs. PPPs are measures that both the project manager and the systems engineer use to track and monitor the project's progress. PPPs are linked directly to the project's performance requirements.

Additional information on a project SEMP is available in Chapter 3: Integrated Technical Planning.

Technical Review Criteria

The technical review criteria are a set of predefined entry and success specifications that contribute to the eventual realization of project objectives. Each technical review employs specific criteria tailored to each phase of the life cycle. These criteria verify the extent of the technical progress made toward solving the identified capabilities shortfall.

Technical Assessment Process Elements

PLAN: Prepare for Technical Assessment

The Technical Assessment process provides the information for which critical project decision are based upon, therefore it is imperative to plan for the process. The two major steps in planning for technical assessment are described below.

Step 1: Develop a Technical Assessment Plan

Before actually performing the technical assessments and reviews, a plan needs to be developed to determine *how*, *when*, and *by whom* these assessments and reviews will be conducted.

At a minimum, a good Technical Assessment plan should address the following:

- Agreed-upon set of measures and technical review criteria
- Reporting format for results from the technical assessments
- Repository for maintaining historical data for trend identification and analysis
- Technical Review list
- Technical Review schedule
- Review and Assessment team members

DO: Monitor and Control Project Progress

Using the details provided in the Information Management plan, technical assessment is performed.

The Technical Assessment activities are as follows:

- Monitor project progress
- Control project progress

Technical monitoring and control is used to generate information or data needed to make a decision. It determines the status of the project and directs project plan execution to guarantee that the project performs as planned and satisfies the technical objectives. Technical monitoring and control are detailed below.

Step 1: Monitor Project/ Program Progress

Within FAA, techniques are used to monitor the technical progress of a project. **Technical Performance Measurement (TPM)** is the key technique used to monitor and assess the technical progress of an FAA project. **Program Performance Measurement (PPM)** is the key technique used to monitor and assess the progress of a project, but for non-technical measures. The TPPs and PPPs, identified in the project SEMP, are the major inputs to a TPM and PPM project respectively. A description of TPM and PPM follows.

Technical Performance Measurement (TPM) – TPM is a process to continuously assess and evaluate the adequacy of architecture and design, as they evolve, to satisfy project requirements and objectives. TPM quantitatively pinpoints emerging design deficiencies and monitors progress relative to satisfying requirements and developing trend information to assess project risks. In a TPM project, TPPs are the measures used to assess and monitor the technical progress of a project.

According to the INCOSE Handbook, in the absence of TPM with well defined TPPs, a project manager would have to rely on cost and schedule status, with perhaps the verbal assurance of the technical staff and project team members to assess the technical progress. This can result in a project being completed on time and within budget, without meeting all key requirements or satisfying technical objectives. With that, the use of TPM is critical to successfully monitoring the technical progress of a project.

Program Performance Measurement (PPM) – PPM is a process to continuously assess and evaluate the adequacy of the project to remain "on-track." PPM is used to track the status of meeting the selected program performance requirements.

The most common application of PPM is the use of **Earned Value Management (EVM).** EVM is a management technique for integrating cost, schedule, TPM, and risk management. An EVM system is established to objectively define the program baseline cost objectives and track them against performance and schedule. For EVM to be effective, planning, budgeting, and scheduling the authorized work scope must be accomplished in a time-phased plan. EVM provides an objective measure of performance, enabling trend analysis and evaluation of costs and schedule estimates at completion for multiple levels and stages of a project.

Whether TPM, PPM, or another technique is used, the progress of a project must be monitored and assessed. The results of these assessments are recorded, reported, and analyzed in accordance with the format established in the Technical Assessment plan.

Step 2: Control Project Process

In FAA, mechanisms are used to control the project progress. As stated earlier, mechanisms are control gates that assess the progress of the system against criteria established for a given point in the system's life cycle. They are used to determine if the current phase of work has been completed and if the team is ready to move to the next phase of the life cycle. The Technical Review Criteria is the major input to this step, as it contains the entrance and exit criteria for each phase of work. The Systems Engineering gates are typically in the form of technical reviews.

Technical Reviews

Technical Reviews assess the maturity of a project. Technical reviews, which are scheduled at strategic points within the development cycle, employ specific criteria tailored to the development effort. A well-structured technical review includes defined entry criteria, a basic set of common steps for every review, a predefined set of outcomes expressed in terms of exit

criteria, and a set of metrics to measure success. Figure 9-2 depicts the Product Development process which details the various reviews during the life cycle as they relate to the AMS phases. Chapters 19-26 elaborate on each AMS phase.

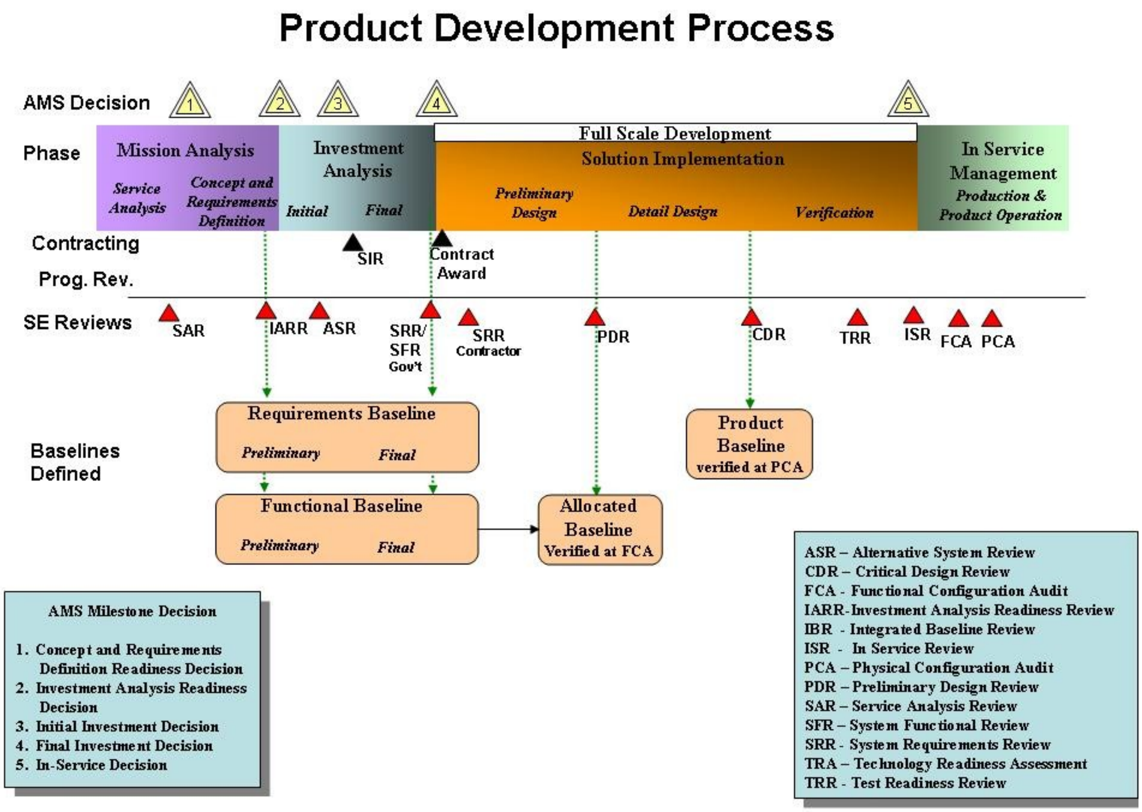


Figure 9-2. Product Planning Process

A good technical assessment strategy addresses all of the prerequisites for conducting a technical review. Each review will have its own scope and objective; however, the inputs and outputs will generally remain the same from review to review and will simply mature from their status at the previous review. Table 9-1 lists typical inputs and outputs, sometimes referred to as entrance and exit criteria respectively, for a technical review.

Technical Review Entry and Exit Criteria		
Entry Criteria (Inputs)		**Exit Criteria (Outputs)**
Previously completed documents and products		Approved design documents
Service-Level Mission Need (SLMN)		SLMN and gap analysis
SEMP		SEMP
Requirements Documents		Requirements Documents
Architectures		Architectures
TPPs and/or PPPs		Verification plans
Constraints		Updated Plans
Risk Mitigation Plans		Updated Risk Mitigation Plans
Test Plans		Test reports
Design Analysis Report (DAR)		Risk Management Reports
Functional analyses		Review Minutes
TPM reports		TPM reports
Test, evaluation, verification, and validation reports		Action item and issue documentation

Table 9-1. Technical Review Entry and Exit Criteria

Technical Reviews in the AMS

FAA has established a set of reviews to support its life cycle model, the AMS process. Each is described below, in the order in which they occur.

- **Integrated Baseline Review (IBR) –** IBRs are intended to provide a mutual understanding of risk inherent in contractor's performance plans and underlying management control systems. Project managers must conduct IBRs on contracts with EVM requirements. IBRs are an essential element of a project manager's risk management approach.
- **System Requirements Review (SRR) –** SRRs clarify the functional, performance, test, and interface requirements contained in the contract and specification. Both the service team and the contactor are involved in SRR. The SRR is complete when the service team determines that action items resulting from the review are sufficiently completed. The System Specification, System/Segment Specification, and Interface Control Documents are typically reviewed during a SRR. The products of functional analyses and trade studies may also be reviewed.

- **System Design Review (SDR) –** SDR evaluates the optimization, traceability, correlation, completeness, and risk of the system-level design to fulfill system functional baseline requirements. SDRs occur when the design definition effort has proceeded to the point where system characteristics are defined and configuration items are identified. Configuration Items are explained in Chapter 7: Configuration Management. The service team determines when this review is complete.
- **Software Specification Review –** Software Specification Review ensures that all segment and Interface Control Document requirements are allocated and traced to Computer Software Configuration Items, and that the methods of verifying and validating requirements are reflected in the Software Requirements Specification (SRS). This review is conducted by the service team and the contractor.
  The contractor conducts a formal review of the SRS in accordance with MIL-STD-1521B. The service team reviews the allocation of performance requirements to major architectural components, as well as external and any interface requirements. The service team also evaluates the impact of any proposed changes to the SRS.
  Both the contractor and service teams review the hardware specifications in the Systems Specification to ensure all requirements can be satisfied by the vendor's hardware. Any discrepancies or conflicts must be corrected before proceeding further in development. When problems emerge, it may be possible to implement functionality in software rather than hardware, or it may require a change to the System Specification or program.
- **System Specification Review (SSR) –** SSRs formally review configuration item requirements as specified in the hardware and software specification. Its purpose is to establish the allocated baseline for preliminary design by demonstrating the adequacy of hardware and software requirements specifications. The SSR is complete when the services team determines that action items resulting from the review are sufficiently completed.
- **Preliminary Design Review (PDR) –** PDR determines the conformity of functional characteristics of the design to baseline requirements. The service team conducts this review.
  The PDR represents approval to begin detailed design. It is complete when the service team determines that action items resulting from the review are sufficiently completed and the contracting officer authorizes the contractor to proceed. Each PDR must ensure the process used to arrive at the functional and performance requirements for each Configuration Item is rigorous and complete. Each must also establish an audit trail from user requirements to the functional baseline, substantiating changes as necessary.

- **Critical Design Review (CDR) –** CDRs evaluate the contractor's product design. The CDR is performed by the service team. It is conducted for each HWCI and CSCI when all engineering drawings are complete. CDRs determine whether the detailed design meets the specified requirements in the appropriate developmental baseline and whether the design is complete and ready to be implemented via detailed software code and test. The CDR is complete when the service team determines the action items resulting from the review are sufficiently completed.
- **Test Readiness Review (TRR) –** TRRs are multi-disciplined reviews that ensure that the subsystem or system under review is ready to proceed to a system-level development test. The TRR determines the completeness of test procedures and their compliance with test plans and descriptions.
- **Production Readiness Review (PRR)** – PRRs determine if production engineering problems have been resolved, adequate planning accomplished, and the design is ready for production. A PPR evaluates the complete production-configured system to determine if it correctly and completely implements all system requirements and that those requirements are traceable to the final production system.

CHECK : Check Technical Assessment Activities

The Technical Assessment process checks to make sure that the project progresses as planned and that all the other life cycle activities are completed correctly, but in order for the technical assessment process to be effective, it must also be checked. The technical assessment process has close relationships to the other technical management areas, most importantly Decision Analysis (Chapter 10). The information generated during the technical assessment process is used to decide when corrective actions need to be taken and which one to choose, so it is imperative that the information being reporting is accurate.

Technical Assessment Checklist to consider:

- ✓ Version of review and assessment criteria. It is critical to use the most recent versions to perform reviews and assessments.
- ✓ Assessment and review date and objective. Make sure the correct reviews are being completed at the correct time in the life cycle. Completing a review with insufficient information could unnecessarily yield negative results.
- ✓ Status of all team members and stakeholders. Maintaining constant communication with team members and stakeholders is important to process and project success.

- ✓ Any and all critical areas. Remember, additional critical areas can arise as the project develops.

ACT: Update as needed

The technical assessment activities may result in the need for change; those changes are made during this phase. Keep the most recent version of the assessment and review documentation to optimize the impacts of the process. Update all documents as needed.

Outputs

The primary outputs of the technical assessment PDCA cycle are the assessment and review reports. These reports are used to make decisions pertaining to the project in question as well as to formulate trend reports and make risk predictions.

Interdependencies

Technical Planning
Life Cycle Management
Configuration Management
Decision Analysis

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

10 – Decision Analysis Process

Introduction

The Decision Analysis process identifies the most optimal solution among a set of viable alternatives. Decision Analysis uses a variety of tools, methods, and procedures to identify and assess decision criteria and alternatives to meet those criteria, resulting in the most-balanced decision. This process quantifies the consequences of selecting various alternatives in terms of metrics that are traceable to stakeholder expectation and overall project objectives. The Decision Analysis process provides a structured methodology for decision-making throughout the life cycle.

The Decision Analysis process supports decisions at any phase of the project's life cycle. It can be applied to make very high-level decisions as well as much more technical, lower level decisions. Decision Analysis will be very important for the formal decision gates during the AMS life cycle and more information on AMS is available in Chapters 19-27 of this manual. Additionally, decision analysis will also be helpful in making less formal decisions. Decision Analysis employs a number of tools and techniques to reach a decision, most notably Trade Studies, described later in this chapter. Cost, reliability, supportability, testability, survivability, and compatibility are a few examples of the types of criteria evaluated during the Decision Analysis process. The Decision analysis process selects the best-value solution, best value to the government, and the best value to a set of requirements from a technical, cost, or schedule point of views.

Decision Analysis occurs during the "Act" phase of the PDCA cycle (Plan, Do, Check, Act) for the Technical Management processes. It is an iterative process and begins whenever the need for a decision arises. It is implemented to ensure that the most beneficial course of action is taken, only after adequate planning, doing, and checking to confirm the need for the decision. The Decision Analysis process directly supports all of the systems engineering processes and is used when the need for change or corrective actions have been identified during the various Technical Assessments and reviews. Chapter 9 details the technical reviews that occur during FAA's AMS life cycle.

The Decision Analysis PDCA cycle is depicted in Figure 10-1. The project manager and system engineer work together to determine when it is appropriate to make a decision, and the Decision process analysis PDCA cycle is triggered by the need for a decision. They will also work together to tailor the process accordingly to meet the need of the particular decision. The primary outputs of the Decision Analysis process are the trade study

report with an executive summary and a design/manufacturing decision document.

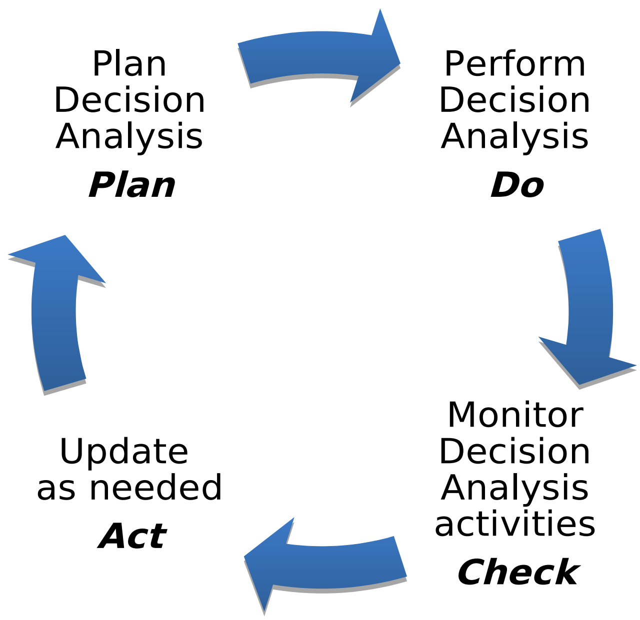


Figure 10-1 Decision Analysis PDCA Cycle

Objective

The Decision Analysis process provides an objective evaluation of alternative solutions when decisions need to be made as to ensure that the optimal solution is selected.

Inputs

There are a number of inputs to the Decision Analysis process. They vary project to project and greatly depend on the scope of the decision. The Decision Analysis process inputs may be divided into 2 categories: **Decision Analysis Governance** and **Decision Information**. Each is described below.

Decision Analysis Governance

Decision Analysis Governance refers to any and all documentation the Decision Analysis PDCA cycle activities must comply with. They are the controls and enablers that govern the Decision Analysis process activities for a particular decision. Decision Analysis governance may constrain alternative solution options, decision criteria, and in some cases define

project budget and schedule. It will be imperative to reaching the most optimal decision to make sure that the Decision Analysis PDCA activities are conducted in compliance with the available governance and guidance for that decision. Some examples of Decision Analysis Governance include:

- FAA policy, procedures, orders
- Standards
- Program policy and procedures
- FAA and organizational agreements
- FAA legislations
- FAA and Project SEMPs, which include the Decision Analysis Plan

Decision Information

Decision Information refers to any and all information pertaining to the decision of interest. These will vary project and project and decision to decision. The scope of the decision will determine what these will be. Because of the interconnections between the SE processes and the impacts that decisions made early in the life cycle can have on outcomes later in the life cycle, it will be very crucial to use other technical management processes, such as Information Management (Chapter 8) and Configuration Management (Chapter 7) to keep the Decision Information organized. Some examples of Decision Information include:

- Decision Requests
- Assumptions and constraints pertaining to the decision
- Identified alternatives
- Project goals and objectives
- User needs
- Concept of Operations
- Requirements Documents
- Enterprise Architecture
- Design Analysis Reports
- Analysis Criteria

Decision Analysis Process Elements

PLAN: Plan Decision Analysis

Decision Analysis planning aids in ensuring that the best choice is selected when alternatives exist. Conducting upfront planning prevents the project manager from committing too early to a design that may not be cost effective or meets all of the systems requirements. Decision Analysis requires the participation of various interdisciplinary skills in an integrated manner with the objective of producing an optimum design further justifying

the importance of the planning phase. Developing a Decision Analysis plan is the major step required to plan for decision analysis.

Step 1: Develop a Decision Analysis Plan

The Decision Analysis plan dictates how the decision analysis process activities will be implemented for a particular decision. The available Decision Analysis governance for the decision of interest will be used to develop the plan to ensure that the process activities are performed in compliance with the governance. The Decision Analysis plan can be found in the SEMP for the project of interest. More information on a SEMP is available in Chapter 3: Integrated Technical Planning.

At minimum, a good Decision Analysis plan should address the following:

- Formality of the decision analysis process. Some decisions may not be as formal as others
- What needs to be documented throughout the process
- Roles and responsibilities for decision making team
- Schedule determining when decisions need to be made, when possible

DO: Perform Decision Analysis

Decision Analysis process is performed according to the Decision Analysis plan, found in the SEMP for the project of interest. The formality of the decision determines the rigor and level of detail for which the following activities are performed.

The major tasks required to perform decision analysis are as follows:

1. Identify and Justify the need for the decision
2. Determine the scope and ground rules of the decision
3. Define Evaluation Criteria and Weighting Factors
4. Select Alternative Solutions
5. Evaluate Alternatives
6. Perform Sensitivity Analysis
7. Review Results and Form Conclusions

Each step is described below.

Step 1: Identify and justify the need for the decision

The Decision Analysis process begins only when the need for a decision is identified. A lot of resources are used during the Decision Analysis process therefore it is important that it only be performed when a need for a decision

really exists. Performing the decision analysis process unnecessarily can cause, amongst other things, major schedule delays and cause a project exceed the allotted budget. Identifying and justifying the need for a decision upfront reduces a project's susceptibility to technical, schedule and cost risks. Some reasons to make a decision hence triggering the Decision Analysis process include the need to:

- Choose among alternative design and implementation strategies and solutions based on architecture, performance, and cost in order to meet stakeholder requirements
- Recommend commercial, off-the-shelf (COTS) products for acquisition
- Perform make versus buy versus lease analyses
- Recommend a supplier for service
- Document and justify the selection of a solution for a systems requirement
- Reduce risk

Step 2: Determine the scope and ground rules of the decision

After identifying the need for a decision, the next step is to understand the goals and scope of that decision. All the material gathered during this step regarding the particular decision is considered Decision Information and will be major inputs to the "Do" phase of the Decision Analysis PDCA cycle. Maintaining communication with the decision stakeholders is crucial to successfully complete this step. Understanding the viewpoints of all the decision stakeholders in order to clearly define the key issues that the decision needs to address is crucial.

Achieving consensus with all decision stakeholders regarding the real problem to be resolved saves significant time in the overall process. It makes completing subsequent tasks much easier. Identifying and considering things such as previously developed hardware and software components as well as COTS hardware and software acquired for the particular system needing the decision will also be helpful in understanding the scope of the current decision.

Step 3: Define Evaluation Criteria and Weighting Factors

Evaluation criteria and weight factors are used to judge the selected alternatives. They provide the basis for assessing alternative solutions. Evaluation criteria define "what matters" and weight factors define "how much" a criterion matters regarding a specific decision. Defining evaluation criteria and their associated weights require considerable engineering judgment and interaction with the decision stakeholders. The Decision Analysis strategy for the decision of interest should, at a minimum, identify the relevant stakeholders.

The systems engineers will work with the decision stakeholders to identify the correct evaluation criteria for the decision of interest. They will decide those things that are mandatory ("must haves") for a potential solution versus those things that are "nice to have". Typically, the evaluation criteria are determined by the requirements that the final solution selected needs to meet. Although not always possible, evaluation criteria should be measurable. Expressing evaluation criteria in measurable terms, where applicable, makes judging alternatives against each other much easier as well as identifying those alternatives that do not fulfill the selected criteria. The following evaluation criteria are applicable to a wide range of decisions:

- Development cost
- Life cycle cost
- Requirements compliance
- Functional
- Performance
- Operational
- Programmatic
- Technical risk (Maturity)
- Reliability, Maintainability, and Availability (RMA)
- System safety
- Human Factors
- Electromagnetic environmental effects
- Hazardous materials
- Budget risk
- Schedule risk
- Operational complexity
- Vendor assessment
- System maturity
- Development support tools
- Test support tools
- Development team familiarity with candidate hardware and software
- Quality of logistics support

Assigning weight factors can be a difficult task and can be very subjective. Not all evaluation criteria will have the same importance and the same criterion can have several different weight factors depending on the scope of the various decisions. The systems engineer will be responsible for ensuring that the correct weights are assigned to the selected evaluation criteria, while the project manager will be responsible for ensuring consensus among all the decision stakeholders. Weight factors can be assigned using a simple 1 to 10 rank, with 10 identifying the most important evaluation criteria, or by using a percentage approach in which each criterion is weighted a percentage and the sum of each criterion's percentage equals 100. Quality Function Deployment (QFD) and Decision Analysis Matrix are some additional tools that can be used to define the evaluation criteria and weighting factors. Figure 10-2 is an example of a Decision Analysis Matrix.

Decision Factors / Alternatives	Decision Factor 1		Decision Factor 2		...	Decision Factor n		Total Weighted Score
	Weight = 1		Weight = 1.5		...	Weight = 2.5		
	Score	Weighted Score	Score	Weighted Score	...	Score	Weighted Score	
Alternative 1	7	21	4	6	...	8	20	47
Alternative 2	8	24	10	15	...	10	25	64
⋮	⋮	⋮	⋮	⋮	...	⋮	⋮	⋮
Alternative n	10	30	5	7.5	...	12	30	67.5
Alternative n+1	⋮	⋮	⋮	⋮	...	⋮	⋮	⋮

Figure 10-2 Decision Analysis Matrix Sample

Defining evaluation criteria and assigning their respective weighting factors often requires several iterations before the final criteria and weight factors are determined, but it is a very important step. The most critical criteria are assigned large weight factors and selecting alternatives that meet those criteria, while also not wasting resources to perform analysis on those options that do not meet those criteria, will result in an overall better implementation of the Decision Analysis process.

Step 4: Select Alternative Solutions

The next step is to select a set of viable alternatives for the decision of interest. Most decisions will have multiple options, while others will only have one. Trade publications, prospective bidders for service contractors, technical staff, stakeholders, and managers, as appropriate, are helpful resources in developing a set of alternatives that may potentially achieve the goals and objectives of the system (*e.g.*, architecture, designs, COTS products).

When numerous possible alternatives are identified, a detailed analysis of each one may not be cost effective and the most beneficial use of resources; therefore down-selection of candidates is recommended. On average, four to six alternatives should be selected for further analysis, from which the final solution will be chosen. Identifying high-risk alternatives and those alternatives with questionable feasibility or high life cycle cost helps reduce the number of alternatives to be analyzed. Screening the alternatives against the evaluation criteria also eliminates alternative candidates. Therefore, those options that do not meet, at a minimum, the essential

evaluation criteria, can be identified and eliminated as early as possible. It is important to document all alternatives considered. A decision analysis matrix (Figure 10-2) can be used to down-select candidate solutions and show how well the alternatives meet the evaluation criteria selected in Step 1.

Step 5: Evaluate Alternatives

The set of alternatives identified in Step 2 are further analyzed to determine how well they satisfy the evaluation criteria selected in Step 1. A variety of tools/techniques and methods can be used to evaluate the alternative solutions. The scope of the decision, the evaluation criteria, and the available resources all need to be considered when selecting an evaluation technique and method for a particular decision.

Some examples of evaluation tools are:

- Modeling and Simulation
- Trade Studies
- Decision Trees
- Influence Diagrams

A trade study is the most commonly used evaluation tool in FAA. It is a key tool in developing designs that meet stakeholder requirements in the most cost efficient manner possible. Trade studies are a crucial part of systems engineering and are conducted within and across disciplines to support decisions at any phase of the project's life cycle. They also provide an objective determination of comparative metrics for various system options.

Conducting trade studies involves evaluating two or more alternatives to select a preferred option. Trade studies may be formal or informal, depending on when in the life cycle they are conducted. They are necessary for making decisions regarding complex systems with multiple possible solutions.

Using the evaluation tool appropriate for the decision of interest, typically trade studies, the alternative solutions are analyzed to quantify the outcome variables by computing estimates of system effectiveness, underlying system performance or technical attributes, and project cost.

Some evaluation methods, used in conjunction with an evaluation tool are:

- Baseline Reference Method
- Relative Rank Method
- Cost Assessment Method

Baseline Reference Method

The baseline reference method involves evaluating alternative solutions against the baseline (or legacy design or other reference) using the selected evaluation criteria. This method requires a team effort of all disciplines participating in the decision. Each alternative is given a rating and all decision stakeholders must agree on the rating assigned to each candidate solution. Generally (+) is used for an alternative clearly better than the baseline, (-) for alternatives clearly worse than the baseline, (S) for same as baseline, and (U) for unacceptable as the baseline.

Relative Rank Method

The relative rank method evaluates each alternative against the selected criteria and establishes a ranking for each criterion. Weighting of the criteria is defined by category, while the alternative solutions are graded in their appropriate columns according to scaling factors over a range of 0 to 4. The average ranking within each category is multiplied by the criteria weighting to determine a score. Scores are summed across the criteria.

Cost Assessment Method

The cost assessment method is similar to the baseline reference method, except that the alternatives are reduced to rough order of magnitude (ROM) estimates of fixed and variable costs. A refinement of earlier ROM estimates is required to complete the information needed to select the most beneficial solution. Cost is a major factor in selecting among candidate solutions during system design; the costs of development, implementation, and operation especially need to be considered when the life cycle costs of alternatives are evaluated.

The following actions are recommended when evaluating candidate solutions:

- Perform a detailed evaluation of all approved viable alternatives. Record any problems or questions and, if a weighted matrix method is used, finish scoring without reference to weights or flags.
- Evaluate the alternative approaches relative to the evaluation criteria.
- Identify any alternatives with high-weighted score that narrowly failed the pass/fail criteria. Discuss these alternatives with the stakeholders.
- Evaluate cost factors separately from the remaining evaluation criteria throughout the Decision Analysis process.

In some cases, none of the candidate solutions may satisfy all the evaluation criteria. In such cases, it may be necessary to relax one or more of the criteria, investigate additional alternatives, or report to the stakeholder that no entirely acceptable solution has been found.

Step 6: Perform Sensitivity Analysis

After evaluating the alternative solutions, it may be necessary to perform a sensitivity analysis. Sensitivity analysis is used when the candidate solutions are nearly equivalent in scoring, and in some cases, may be required even if the scoring is equivalent.

Recommended actions for performing a sensitivity analysis include the following:

- Analyze all alternatives to determine if the differences between the scores are truly significant and if minor variations in the raw scores and weights might affect the selection. Reference any questions or problems noted by the evaluators. For each alternative, including any solution that is compliant based on redefined pass/fail criteria; determine if any weighted score or total for a group of related weighted scores is sensitive to variation of weights or scores.
- Evaluate the effect on weighed scores of varying weights. Weights determined by compromise amongst stakeholders can cause such variation.
- Evaluate the sensitivity of weighted scores to variation of scores. If a number of evaluators have evaluated the alternatives against a given criterion, the range of scores recorded provides useful guidance for such variation.
- Record the ranges of scores and weights evaluated for each criterion. Compute the upper and lower bound for weight scores. Document the data in a matrix corresponding to the score and the weighted score matrices.
- Determine if any of the variations are large enough to require special attention. This can be accomplished by inspecting or using a suitable statistical test.
- Evaluate the effect on weighted scores total, including or excluding criteria flagged as non-critical.

Common outcomes of the sensitivity analysis and review of results include the following:

Case 1: One alternative emerges as the optimal choice if it meets all the critical requirements, has the highest weighted score, and has the lowest cost

Case 2: More than one alternative is acceptable.

Case 3: No single, entirely satisfactory alternative is found.

Case 3 is the most difficult to resolve. A review of evaluation criteria, especially pass/fail and critical criteria, may indicate that no satisfactory alternative has been identified by the analysis. In this case, engineering

judgment and discussions with the stakeholder shall be used to define additional alternatives or to accept a less-than-optimal alternative.

Step 7: Review Results and Form Conclusions
This step typically presents one alternative as the best option after having evaluated and analyzed all of the applicable candidate solutions. The decision analysis team then makes recommendations to the defined FAA decision authority, which makes the final decision. All assumptions, constraints, and changes from the baselines used during the analysis should be documented and formatted in a Decision Analysis Report (DAR), which is detailed in the Outputs section, below.

CHECK: Check Decision Analysis Activities

The Decision Analysis process ensures that the optimal solution is chosen when alternatives exist; therefore, checking to make sure the decision is based on accurate information is imperative to obtaining meaningful results.

Decision Analysis checklist to consider:

- ✓ Accuracy, relevance, and validity of decision information
- ✓ Accuracy , relevance, and validity of decision guidance
- ✓ Evaluation Methods: Check to ensure that they have been performed correctly
- ✓ Analysis Reports
- ✓ Evaluation Criteria

ACT: Update as needed

This phase is saved for any changes that need to be made following reviews of decision analysis activities and associated information. This includes obtaining any additional information for further analysis and any revisions to evaluation and preliminary conclusions.

This phase can be repeated as many times as needed and in some cases, may not need to be performed at all assuming the Decision Analysis process was performed correctly the first time.

Outputs

There are two major outputs of the Decision Analysis process:

Decision Analysis Report (DAR)

A decision analysis report (DAR) is prepared for each decision. The report documents the decision results and provides traceability to decisions made earlier in the project’s life cycle. It provides the traceability needed to

substantiate design and configuration changes to the baseline design and also documents the decision-making process that selected one alternative over another. It is recommended that the DAR format be standardized wherever possible to satisfy individual project needs. At a minimum, a DAR should include the following:

- Clear problem statement
- Identification of affected requirements
- Ground rules and assumptions
- Decision criteria
- Resource requirements statement to accomplish the decision
- Schedule to accomplish (actual and proposed)
- Evaluation of all potential solutions and screening matrix
- Comparisons of alternatives using decision criteria
- Technical recommendations from the decision analysis team
- Documentation of any decision leading to the final technical recommendation

Design/Manufacture Document

Once the DAR is approved, the design decision/manufacturing document is produced, outlining the impacts and actions necessary to implement the selected alternative into the baseline configuration. In general, this document describes the rationale required to substantiate the change. The design decision document is submitted to the appropriate control authority to authorize implementation into the baseline configuration.

Both outputs will be under Configuration Management (see Chapter 7 for more details on this process) and the control authority is required to maintain the DAR and Design/Manufacturing decision document for the entirety of the project's life cycle.

Interdependencies

Configuration Management
Integrated Technical Planning

References

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

11 – Operational Concepts Process

Introduction

The Operational Concepts process defines the concept of operations for a capability that can provide the services needed by users and other stakeholders in a defined environment. A stakeholder is any individual or organization with a legitimate interest in the system (INCOSE 2010). In essence, the process helps define why a new capability is needed. It initiates the technical activities for the engineering (or reengineering) of a system, regardless of complexity, and it explores what is needed by stakeholders and the operational environment. The process identifies stakeholders, or stakeholder classes, involved with the capability throughout its life cycle, and their needs, mission goals, expectations, and desires. It analyzes and transforms these needs and goals into a common set of stakeholder expectations that expresses the intended interaction the capability will have with its operational environment and that is the reference against which each resulting operational service is validated (ISO-15288 2008).

The project manager and systems engineer work with the user to establish and refine operational needs, attributes, performance parameters, and constraints that flow from the described capabilities, and then ensure that all relevant requirements are addressed. The focus of the process is to gather and translate stakeholder needs into operational requirements, which include performance parameter objectives and thresholds, affordability constraints, and technical constraints.

The Systems Engineering (SE) sub-processes in the Operational Concept process are as follows:

1) Capability Analysis
2) Stakeholders Analysis
3) Operational Analysis

The Capability Analysis sub-process validates the agency's need or shortfall that requires a new capability.
The Stakeholder Analysis sub-process elicits inputs from relevant stakeholders and translates the inputs into documented expectations.
The Operational Analysis sub-process establishes the operational concepts and associated scenarios for the proposed capability.
Although presented sequentially, these sub-processes are conducted in parallel and should be reiterated as new information arises.

The output of the process is documented in the Concept of Operations (CONOPS). A CONOPS document quantitatively and qualitatively describes the needs of the stakeholders and depicts the new system from the user's point of view (ISO-15288 2008).

Objective

The Operational Concepts process defines the stakeholders' needs and goals for a capability in a defined environment.

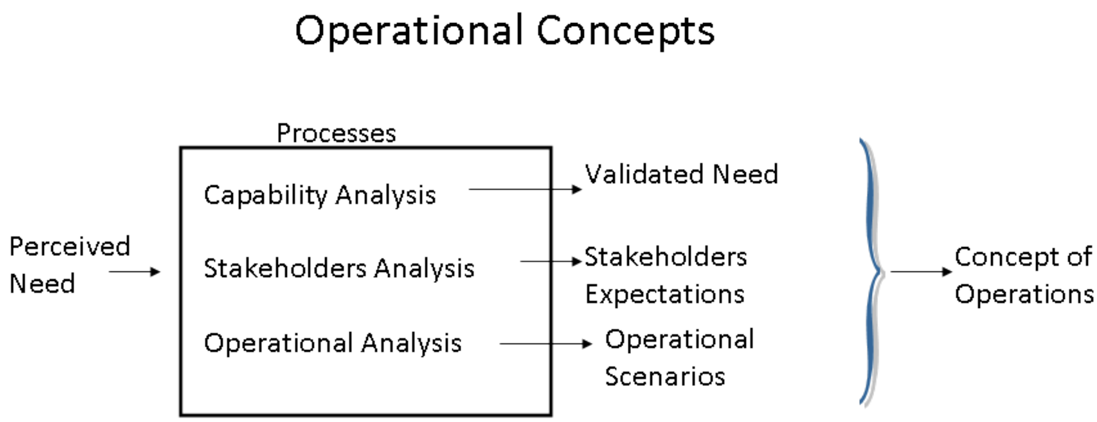


Figure 11-1. Input, Processes, Output Diagram

Inputs or Essential Criteria

The Perceived Need in the figure above is the input to the Operational Concept process and includes any program directives. These directives will vary by program and can take many forms, such as gap studies or need-related white papers. Additionally, other inputs may include—but are not limited to—National Airspace System (NAS) Requirements, Federal Aviation Administration (FAA) Enterprise Architecture (EA), and other agency artifacts.

Essential Inputs

The primary input to the Operational Concepts process is the following:

- Perceived need, *e.g.*, shortfall; gap; or mission goal

Systems engineering commences when a mission goal or need is perceived in the form of a new or improved capability, or lack thereof. This need may be the result of a gap analysis, operational improvement, executive directive, or other defined problem. A need may be constructed based on new laws, ordinances or legislative directives. It can develop into a shortfall or absence of a "required" functionality, capability, performance, security, safety, and/or technology criteria. A particular community or invested group

of stakeholders generate and identify needs. Needs vary, depending upon the magnitude and requirements of a particular task or project. The need may be to eliminate noted vulnerabilities or levels of risk, or it may be to enhance or replace existing systems.

Process Components

There are three main sub-processes in the accomplishment of the Operational Concepts process, as follows:

- Capability Analysis
- Stakeholders Analysis
- Operational Analysis

The Operational Concept process begins with Capability Analysis but otherwise the three sub-processes are iterative and may occur in parallel. Elsewhere, such as the Department of Defense (DoD) and the International Council on Systems Engineering (INCOSE), Stakeholder Analysis has been called Concept Exploration, and Operational Analysis has been called Concept Development.

Capability Analysis

The Capability Analysis sub-process defines and validates agency needs, goals, and some problem statement in the form of capabilities, gaps, and opportunities. Examples in the FAA include an identified agency shortfall, a service gap, or a Congressional directive, just to name a few. Problem statements in the form of capabilities, gaps, and opportunities may come from FAA strategic planning documents, NAS requirements, NAS Enterprise Architecture, NAS ConOps, the NAS Enterprise Architecture Road Maps, and any other FAA directive.

The result of the Capability Analysis sub-process is a validated need or validated problem statement. It is recommended that the definition of the needs be balanced with an analysis of their effects on the overall system design and performance as well as on human engineering; knowledge, skills, and abilities; availability; maintainability; reliability; safety; and training requirements of the humans required to support lifecycle processes (IEEE 1220 2005).

Stakeholders Analysis

The goal of the Stakeholder Analysis sub-process is to describe a set of documented stakeholder expectations and needs, and use that set in the development of the system's requirements in later processes. The stakeholders' expectations express what the stakeholders want the system

to accomplish (functional requirements). Also, the stakeholders provide how well each function will be accomplished (performance), the natural and induced environments in which the system will operate or be used, and any known constraints (IEEE 1220 2005).

Stakeholders can be an enterprise, organization, or an individual having an interest or a stake in the outcome of the engineering of a system (EIA-632 1999). Examples of stakeholders include project and program managers, systems engineers, Congress, users, operators, and FAA contractors. It is important that the list of stakeholders be identified early in the process, as well as the primary stakeholders who will have the most significant influence over the project (NASA 2007).

These stakeholder expectations may be expressed in the stakeholder's terms and may be nontechnical descriptions. Stakeholder needs, expectations, constraints, and interfaces comprise the stakeholder expectations document (CMMI-DEV V1.2 2006). These stakeholder expectations are the reference against which each resulting operational service is validated (INCOSE 2010). However, eliciting stakeholder expectations goes beyond collecting information by proactively identifying additional requirements not explicitly provided by the stakeholders. These additional sources of requirements include policies, standards, environmental requirements (*e.g.*, laboratories, testing and other facilities, and information technology infrastructure), technology, legacy systems, and the capabilities and operational characteristics of users (CMMI-DEV V1.2 2006).

All these early necessities are expressed in terms of a model that may be textural or formal, that concentrates on system purpose and behavior, and that is described in the context of the operational environment and conditions (ISO-15288 2008). It is useful to cite sources, including solicitation documents or agreements, and where possible, their justification and rationale. Also cite the assumptions of stakeholders and the value they place on the satisfaction of their requirements. For key stakeholder needs, the measures of effectiveness are defined so that the operational performance can be measured and assessed (ISO-15288 2008).

Operational Analysis

The Operational Analysis sub-process establishes the operational concepts and associated scenarios for the proposed capability (CMMI-DEV V1.2 2006). The goal of Operational Analysis is to ensure the proposed concepts fully satisfy the strategic objectives and defined service needs of the Agency. Based on the stakeholder's input, the engineer can begin to formulate the proper high level requirements needed to verbally describe the system. In

the case where there is an existing system and the need is an enhanced functionality or capability, the systems engineer would most likely utilize the legacy requirements for the system (if available) in addition to the stakeholders' input.

Operational Analysis uses the stakeholder expectations to produce an operational architecture in the form of context diagram(s), use cases, sequence diagrams, and any other analysis diagrams that depict the operational scenarios. These operational scenarios define the range of the anticipated uses of the needed capability, and define expected interactions with the environment and other systems; human tasks and task sequences; and physical interconnections with interfacing systems, platforms, or products (IEEE 1220 2005). All results of the Operational Analysis are validated with the appropriate stakeholders.

While the stakeholder expectations express the intended interaction between the system and its operational environment, the operational diagrams are analysis tools that examine the operation of the capability in its intended environment. The operational diagrams help identify expectations and requirements that may not have been formally specified by any of the stakeholders, *e.g.*, legal, regulatory, and social obligations. Consequently, the system boundaries are defined and captured, usually in a context diagram.

The context diagram or equivalent defines which system elements are under design control of the project and which fall outside their control. Also it defines the expected interactions among system elements with external and higher-level interacting systems outside the system boundary (IEEE 1220 2005). In addition to the context diagram, the context of use for the capability is identified and analyzed. Operational Analysis identifies the activities that users perform to achieve system objectives, the relevant characteristics of the end users of the system (*e.g.*, expected training, degree of fatigue), the physical environment (*e.g.*, available light, temperature) and any equipment to be used (*e.g.*, protective or communication equipment). The social and organizational influences on users that could affect system use or constrain its design are analyzed when applicable (EIA-632 1999; ISO-15288 2008).

Essential Outputs

The primary output of the Operational Concepts process is the Concept of Operations (CONOPS). The CONOPS comprises the outputs from the three sub-processes of Capability Analysis, Stakeholder Analysis, and Operational Analysis.

Concept of Operations

The outputs from the Operational Concepts process are compiled into a CONOPS. The CONOPS describes how a set of capabilities, from the user's perspective, will operate to enable operational improvements or achieve desired objectives for a proposed system. The CONOPS document is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements (*e.g.*, training, facilities, staffing, and maintenance). It describes the user organization(s), mission(s), and organizational objectives from an integrated system's point of view (IEEE 1362 1998). It must involve the input from a broad range of stakeholders, such as operations, maintenance, and management personnel. The document also describes any critical, top-level performance requirements or objectives, both stated either qualitatively or quantitatively, and it describes system rationale as well as the roles, responsibilities, and skill sets needed for operations and maintenance of the implemented system (INCOSE 2010).

Validated Need Output

The Operational Concepts process begins with a perceived need or mission goal, which may be in the form of capabilities, gaps, or opportunities. The needs are documented formally in the Capability Analysis sub-process into a problem statement, which represents the validated need. The need signifies a necessity, want or desire for a new or improved capability based on a real or perceived deficiency (Blanchard and Fabrycky 1998).

Stakeholder Expectations Output

Once the identified stakeholders have expressed their expectations for a new or improved capability, the Stakeholder Analysis sub-process records the expectations, goals, and needs into a stakeholder expectations document. These stakeholder expectations include intended accomplishments of the capability, basic operating characteristics, anticipated usage of the capability, any known reliability requirements, a description of the intended environment of the capability (Blanchard and Fabrycky 1998), and any known reliability or safety requirements.

Operational Scenarios Output

The primary result of the Operational Analysis process is a set of operational scenarios depicting how any capability addressing the problem statement will most likely operate. Output may take the form of context diagram(s), use cases, sequence diagrams, activity diagrams, or other operational diagrams that depict the need in an operational context. The identified stakeholders are documented to show their roles related to the needed capability, which

may be represented in the context diagram or in some stand-alone document.

Description of Diagrams

Unified Modeling Language (UML)
UML is a standardized, general-purpose modeling language with extensions for systems engineering (SysML). Applications to systems engineering support the specification, visualization, analysis, design, verification, and validation of a broad range of systems and systems-of-systems.

Context Diagram
A context diagram shows the system boundaries, external entities that interact with the system, and the relevant information flows between these external entities and the system.

Use-Case Diagram
In the UML, this diagram is a type of behavioral diagram defined by and created from a use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

Sequence Diagram
In UML, this diagram is an interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

Activity Diagram
Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration, and concurrency. In the UML, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

Interdependencies

Configuration Management
Requirements Management
Validation
Human Factors Engineering

Information Security
System Safety

External Sources for More Detailed Information

Section 4.1 "Stakeholder Requirements Definition Process" of the INCOSE Handbook (INCOSE 2010) depicts a similar process as the Operational Concept process.

See http://www.omgsysml.org/ (accessed September 7, 2012) for specifications and tutorials on the OMG's SysML.

Readers interested in learning more on how to write good requirements as well as many of the systems engineering best practices represented in this chapter are referred to the following textbooks**:**

Alexander, Ian F, and Richard Stevens. 2002. *Writing Better Requirements*. New York: Addison-Wesley.

Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.

Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.

Sage, Andew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sage, Andew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sobkiw, Walter. 2011. Systems Practices as Common Sense. Cherry Hill, NJ: CassBeth

References

Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

CMMI-DEV V1.2. 2006. *CMMI for Development, Version 1.2*. Standard. Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute, August.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

IEEE 1362. 1998. *IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document*. Standard. New York: The Institute of Electrical and Electronics Engineers, December 31.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

NASA. 2007. *NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December.

12 – Functional & Performance Allocation Process

Introduction

The Functional & Performance Allocation process examines a system's functions and sub-functions that accomplish the system's operation or mission. While the Operational Concept process defines *why* a new capability is needed, this process focuses on *what* the system does, not *how* it does it. Functional and non functional analyses are conducted at the level needed to support later design efforts, with all operational modes and environments included. Each function required to meet the operational needs of a system is identified, defined, and organized into a functional architecture. Performance and other non-functional conditions are identified in order to fully define system-level requirements. The development of requirements is both iterative and recursive.

The purpose of the Functional & Performance Allocation process is to transform the stakeholder and operational views of desired capabilities into a technical view of a required system (regardless of complexity) that could deliver those capabilities. This process builds a representation of a future system or potential system of systems that will meet stakeholder expectations and that, as far as constraints permit, does not imply any specific implementation. The process results in measurable, system-level requirements that specify what characteristics the system is to possess and with what magnitude in order to satisfy stakeholder expectations (ISO-15288 2008).

As a result of the successful implementation of the Functional & Performance Allocation process (ISO-15288 2008):

- The required characteristics, attributes, and functional and performance requirements for a solution are specified.
- Constraints that will affect the design of a system and the means to realize it are specified.
- A basis is defined for verifying that the system requirements are satisfied.

Although either may be functional or nonfunctional, a requirement differs from a constraint, in that a constraint is imposed on the solution by circumstance, force, or compulsion (IEEE 1233 1998).

Defining, deriving, and refining functional and performance requirements applies to the total system over its life cycle, including its supporting requirements (*e.g.*, security, reliability, maintainability, availability, human factors, environmental). These requirements need to be formally documented in a manner that defines the functions and interfaces and characterizes system performance such that they can be flowed down to hardware and software designers (INCOSE 2010).

The Systems Engineering (SE) sub-processes in the Functional & Performance Allocation process are as follows:

- Perform Functional Analysis
- Develop System Requirements

The output of this process is a systems requirements document, incorporating both functional and performance requirements.

Objective

The Functional and Performance Allocation process refines the problem defined by the Operational Concept process in clearer detail, and it identifies lower-level functions via functional decomposition that should be satisfied by elements of the system design (*e.g.*, subsystems, components, or parts). The result of the functional analysis and performance definition is the derivation of the system requirements.

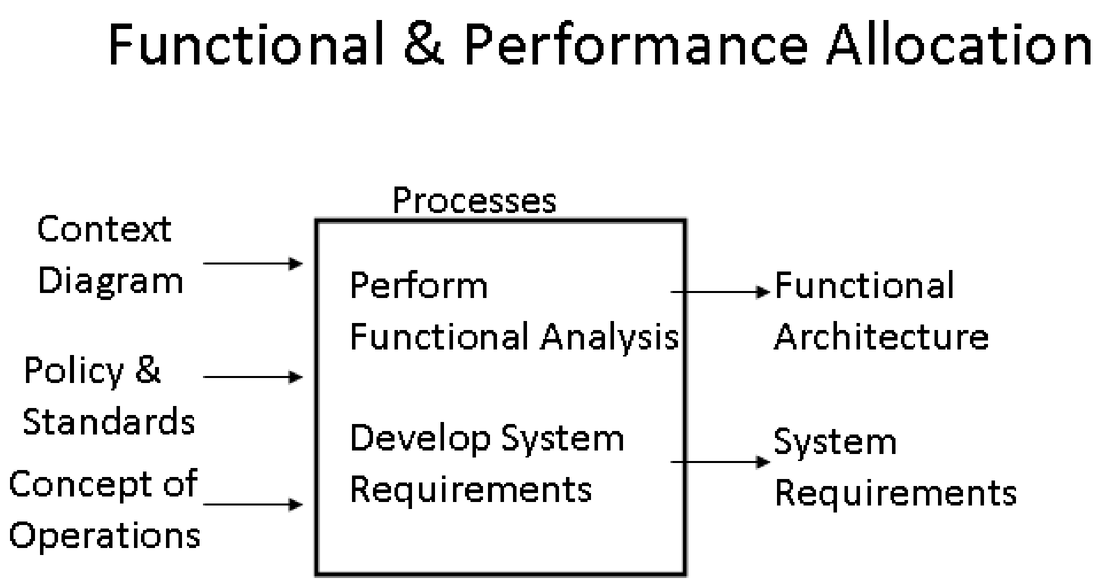


Figure 12-1. Input, Processes, Output Diagram

Essential Inputs

The inputs required for the Functional & Performance Allocation will vary, depending on the scope of a given effort and the iteration of the process. Based on the Operational Concept process output, the primary inputs (at the highest level) are the following:

- Context Diagram
- Other information contained in the Concept of Operations (CONOPS)
- Policy and Standards

Context Diagram

To define the problem from a functional standpoint, one must first review all existing inputs to obtain a complete understanding of the mission and the top-level functions, environments, requirements, imposed constraints, and boundaries. The context diagram shows the expected system boundaries, external entities that interact with the anticipated system, and the relevant information flows between these external entities and the proposed system. Understanding the possible inputs ensures that one will consider the future system's relationship to its environment and to its external systems during development of the primary functions.

Concept of Operations (CONOPS)

The Concept of Operations (CONOPS) document encompasses the results of the Operational Concept process and is intended to describe a new system's operational characteristics from the user's point of view (i.e. stakeholder expectations) (ISO-15288 2008; IEEE 1362 1998). The CONOPS document defines the way the system will be used and involves input from a broad range of stakeholders, such as operations, maintenance, and management personnel. The document also indicates any critical, top-level performance requirements or objectives (stated either qualitatively or quantitatively) and system rationale (INCOSE 2010; IEEE 1362 1998).

It should be noted that the U.S. DoD and others use the term CONOPS to mean how the *enterprise* will operate. They use the term Operational Concept to discuss how the *system* will operate within the context of the enterprise (INCOSE 2010). This manual uses the term CONOPS for both instances but specifically to indicate the output of the Operational Concept phase.

Policy and Standards

All relevant agency policy as well as any applicable industry standards are an input as constraints or passive requirements to the functional analysis and eventual systems requirements.

Process Components

There are two main sub-processes in the accomplishment of the Functional & Performance Allocation process, as follows:

- Perform Functional Analysis
- Develop System Requirements

Perform Functional Analysis (ISO-15288 2008)

The Perform Functional Analysis sub-process establishes and maintains a definition of required functionality (CMMI-DEV V1.2 2006). Functional analysis should be performed without consideration for a design solution (IEEE 1220 2005). There are two primary reasons for conducting a functional analysis. First, it describes the defined problem in clearer detail, and second it decomposes the functions to lower-level functions that should be satisfied by elements of the system design (*e.g.*, subsystems, components, or parts) (IEEE 1220 2005). Model-based systems engineering could be performed as an alternative to functional analysis with similar results in SysML format (INCOSE 2010).

The functions identified through functional analysis are further refined through functional decomposition to provide a basis for identifying and assessing design alternatives. The decompositions result in a set of basic sub-functions, and each sub-function at the lowest level is instantiated in a valid set of requirements. The performance requirements are allocated to sub-functions during the functional decomposition and are the criteria against which design solutions are measured.

The high-level activities performed during a functional analysis are as follows (ISO-15288 2008):

1) Define the functional boundary of the system in terms of the behavior and properties to be provided. The scope of this sub-process includes the system's stimuli and its responses to user and environment behavior. It also includes an analysis and description of the required interactions between the system and its operational environment in terms of interface constraints (such as mechanical, electrical, mass, thermal, data, and procedural flows). The result establishes the expected system behavior, expressed in quantitative terms, at its boundary.

2) Define each function that the system is required to perform. These functions are *what* the proposed system must do to accomplish its operational mission and stakeholder expectations and not *how* it will accomplish them.

3) Define necessary implementation constraints that are introduced by stakeholder expectations or that are unavoidable solution limitations. The allocated constraints include the implementation decisions, based on the structure of the system.

4) Define the external interfaces and all functional interfaces. As system functions are decomposed into more refined functions, interfaces between interacting functions are created. The interfaces are identified and their functional interactions are defined, such as start and end states or inputs and outputs (IEEE 1220 2005). The activity may develop N^2 charts, IDEF0 diagrams, Functional Flow Block Diagrams, SV-4, or any other functional diagram that illustrates the interaction of functions. System requirements depend heavily on abstract representations of proposed system functions and may employ multiple modeling techniques and perspectives to give a sufficiently complete description of the desired system requirements.

5) Verify the results of functional analysis against the Concept of Operations.

6) Validate the results of the functional analysis against the Stakeholder Expectations (IEEE 1220 2005)

Develop System Requirements (ISO-15288 2008)

The Develop Systems Requirements sub-process is conducted to understand the functional and performance behavior of the system under various conditions and to assess the integrity of the functional architecture. While the functional requirements define what the system should be able to do, the performance requirements define how well the functions must be performed to satisfy the system's goals. Analyses should involve the simulation or stimulation of functional models utilizing operational scenarios that expose the models to a variety of stressful and non-stressful situations that reflect anticipated operational usage and environments (IEEE 1220 2005). System requirements must encompass functional and performance components.

The high-level activities performed during the Develop System Requirements sub-process are as follows (ISO-15288 2008):

1) Derive the functional requirements based on the functional architecture.

2) Define the performance or conditions for each function as represented in the functional architecture. These nonfunctional components indicate for the system:

- how well the system, including its operators, is able to perform that function,
- the conditions under which the system is to be capable of performing the function,
- the conditions under which the system is to commence performing that function, and
- the conditions under which the system is to cease performing that function.

Conditions for the performance of functions may incorporate references to required states, rates, and modes of operation of the system.

3) Define necessary performance introduced by stakeholder expectations or are unavoidable solution limitations. These performance requirements or constraints are not allocable to any function, but specify a characteristic of the system, such as speed, aesthetics, reliability, maintainability, availability, etc.

4) Define technical and quality-in-use measures that enable the assessment of technical achievement. These measures include defining critical performance parameters associated with each effectiveness measure identified in the stakeholder expectations. The critical performance measures can be analyzed and reviewed to ensure stakeholder expectations are met and to ensure identification of project cost, schedule or performance risk associated with any non-compliance (IEEE 1220 2005).

5) Verify the requirements to assess the completeness against the validated functional architecture.

6) Validate the requirements to ensure they represent the identified stakeholder expectations and constraints, and to determine whether the full spectrum of possible system operations and system life cycle support concepts have been adequately addressed (IEEE 1220 2005).

The specific goal of this sub-process develops a set of system requirements to use in the design of system components in the Design Solution phase (CMMI-DEV V1.2 2006). These system requirements consist of functional and performance requirements and comprise a validated functional baseline, which is placed under configuration management control. Performance requirements are divided into allocable sets and are directly allocated to functions. Requirements that are not directly allocable should be translated into derived performance requirements, such as fuel capacity, range, engine efficiency, and vehicle resistance, through appropriate engineering techniques (IEEE 1220 2005).

This task includes analysis and definition of safety considerations, including those relating to methods of operation and maintenance, environmental influences and personnel injury. It also includes each safety-related function. These safety considerations contribute to an Operational Safety Assessment, which is part of the Safety Management System. The associated safety integrity, expressed in terms of the necessary risk reduction, is specified and allocated to designated safety-related systems. Applicable standards are used concerning functional safety, e.g., IEC 61508, and environmental protection, e.g., ISO 14001. Another area of consideration is security including those related to compromise and protection of sensitive information, data and material (ISO-15288 2008).

Essential Outputs

Functional Architecture Output

The Functional Analysis sub-process produces a functional architecture. The functional architecture is a hierarchical arrangement of functions and interfaces that represents the complete system. The sub-process moves to a greater level of detail as the identified functions are further decomposed into sub-functions. Functional decomposition reduces complexity by allocating functionality and interfaces to more readily understood and managed sub-level functions. This process is repeated until the system is completely decomposed into basic sub-functions, and each sub-function at the lowest level is instantiated in a valid set of requirements. The interfaces between each of the functions and sub-functions are fully defined, as are the interfaces to the environment and external systems. The functions and sub-functions are arrayed in a functional architecture to show their relationships and internal and external interfaces. The resulting functional architecture may be represented in N^2 diagrams, IDEF0 diagrams, Functional Flow Block Diagrams, SV-4 diagrams, or any other functional diagram that illustrates the interaction of functions.

System Requirements Output

The primary output of the process is the system requirements, which typically involve a functional and performance component. System requirements are the foundation of the system definition and are a primary input to the system design, integration process, and verification processes. Changes in requirements later in the development cycle can have adverse effects on the project. System requirements having both functional and performance aspects ensure the requirements are complete, consistent, and verifiable (IEEE 1220 2005). Therefore, the complete system requirements must include functional and non-functional requirements, such as performance, reliability, maintainability, availability, and other criteria that

can be used to judge the operation of the system (CMMI-DEV V1.2 2006; IEEE 830 1998; IEEE 1233 1998; ISO-15288 2008). Although either may be functional or nonfunctional, requirement differs from a constraint, in that a constraint is imposed on the solution by circumstance, force, or compulsion (IEEE 1233 1998).

Functions are necessary capabilities of a system in order for it to meet the stakeholder expectations and address the documented needs. These functions describe *what* the system must do but do not indicate *how* the system will actually accomplish it. Consequently, a good requirement identifies a process for transforming inputs into outputs.

Performance or non-functions are documented in the form of text, tables, or diagrams. Performance components are characteristics or conditions imposed on a function. For example, “performance” describes how well functions are performed. Consequently, performance components must be clearly defined for each function and documented along with their accompanying function.

Some performance may take the form of global or stand-alone requirements as a result of stakeholder expectations. Often, these non-functional stakeholder expectations take a very non-technical form, such as “easy to use” or “efficiency.” For these stakeholder expectations, a House of Quality Function Deployment or Quality Function Deployment diagram may be employed. Other diagrams that may represent performance and other non-functional requirements include use cases, operational walkthroughs, interviews, surveys, and questionnaires (CMMI-DEV V1.2 2006).

Combining the functional, performance and other non-functional requirements along with any constraints results in a set of well-formed system requirements. A well-formed requirement is a statement of system functionality (a capability) that can be validated, that must be met or possessed by a system to solve the documented need or to achieve a stakeholder objective, and that is qualified by measurable conditions and bounded by constraints (IEEE 1233 1998).

Description of Diagrams

N^2 Diagram

An N^2 diagram or N^2 chart is a matrix structure that depicts the inputs, outputs, and functions of a system. This systems engineering tool is used for tabulating, defining, analyzing, and describing functional interfaces and interactions among system components. The elements of the diagram are at

the same level of hierarchical decomposition. The diagram is constructed so that functions are represented in boxes down the diagonal and illustrate the inputs and outputs between each function (Buede 2000; Grady 2006; IEEE 1362 1998).

IDEF0 Diagram

The Integrated Definition for Function Modeling (IDEF0) is a process for modeling how inputs are transformed into outputs via some function. The resulting artifacts are called IDEF0 diagrams. An IDEF0 diagram can represent any level of system abstraction, and at least two diagrams are needed per system. The first IDEF0 diagram, known as page A-0, depicts the context diagram with the inputs, controls, outputs, and mechanisms for the top-level function of the system. This diagram establishes the scope and boundaries of the system and indicates interacting external systems. The remaining IDEF0 diagrams represent a decomposition of a function from a higher level of abstraction, starting with the function identified in A-0 (Buede 2000).

Functional Flow Block Diagram

Functional Flow Block Diagrams provide a hierarchical decomposition of the system's functions. The diagrams illustrate the control structure that dictates the order in which the functions can be executed at each level of decomposition (Buede 2000).

Data Flow Diagram

The basic constructs of a Data Flow Diagram are the function or activity, data flow, and terminator. The diagram represents the data or information flow between functions. The terminator represents an external system (Buede 2000).

SV-4

The SV-4 is an enterprise architecture artifact that illustrates functions performed by systems and the system data flows among system functions. The results of the functional analysis directly contribute to the development of the SV-4 artifact.

House of Quality Function Deployment or Quality Function Deployment

The Quality Function Deployment (QFD) is a method to facilitate the transformation of stakeholder expectations into requirements. In many cases these requirements are performance requirements, although they do not have to be. Often these stakeholder expectations are subjective and the QFD

is a tool to translate them into well-defined terms (Blanchard and Fabrycky 1998).

Interdependencies

Configuration Management
Validation
Verification
Interface Management
Requirements Management
Human Factors
Decision Analysis
Risk Management
RMA
Information Security

External Sources for More Detailed Information

Section 4.2 "Requirements Analysis Process" of the INCOSE Handbook (INCOSE 2010) depicts a similar process as the Functional & Performance Allocation process.

Readers interested in learning more on how to perform a functional analysis and analyze performance expectations, as well as many aspects of requirements represented in this chapter, are referred to the following textbooks**:**

Alexander, Ian F, and Richard Stevens. 2002. *Writing Better Requirements*. New York: Addison-Wesley.

Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.

Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.

Sage, Andew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sage, Andew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sobkiw, Walter. 2011. *Systems Practices as Common Sense*. Cherry Hill, NJ: CassBeth

References

Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.

CMMI-DEV V1.2. 2006. *CMMI for Development, Version 1.2*. Standard. Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute, August.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

IEEE 1233. 1998. *IEEE Guide for Developing System Requirements Specifications*. Standard. New York: IEEE Computer Society, December 8.

IEEE 1362. 1998. *IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document*. Standard. New York: The Institute of Electrical and Electronics Engineers, December 31.

IEEE 830. 1998. *IEEE Recommended Practice for Software Requirements Specifications*. Standard. New York: IEEE Computer Society, October 20.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

13 – Design Solution Process

Introduction

The Design Solution process describes the system that accomplishes FAA's need, gap or mission goal as defined in the Capabilities, Gaps, and Opportunities statement. As previous chapters focus on why the system is needed and what the system does, this process explains how the system does what it is required to do. The development of the resulting design specification document(s) is both iterative and recursive. Within the Federal Aviation Administration (FAA), contractors primarily conduct this process. The federal government is not supposed to dictate a solution but only a need (i.e. what is required but not how to accomplish it). The contractors respond with proposed solutions, of which the federal government chooses the best one to address its needs.

The Design Solution process identifies systems and subsystems specifications to satisfy the system requirements of the verified functional architecture. The Design Solution process tasks translate the functional architecture into a design or physical architecture that provides an arrangement of system elements and their decomposition, interfaces (internal and external), and design constraints. A preferred solution adhering to the system requirements is selected from a set of alternatives with an understanding of associated cost, schedule, performance, and risk implications (IEEE 1220 2005).

The Systems Engineering (SE) sub-processes in the Design Solution process are as follows:

- Baseline the Design
- Allocate Requirements
- Identify Physical Interfaces

Objective

The successful results of the Design Solution process include the following (ISO-15288 2008):

- A physical design baseline is established.
- An implementable set of design specifications that satisfy the system requirements are captured.
- The interface requirements are incorporated into the physical design solution.

In addition to these primary objectives, this process provides the following:

- The traceability of the design solution to system requirements is established.
- A basis for verifying the system elements is defined.
- A basis for the integration of system elements is established.

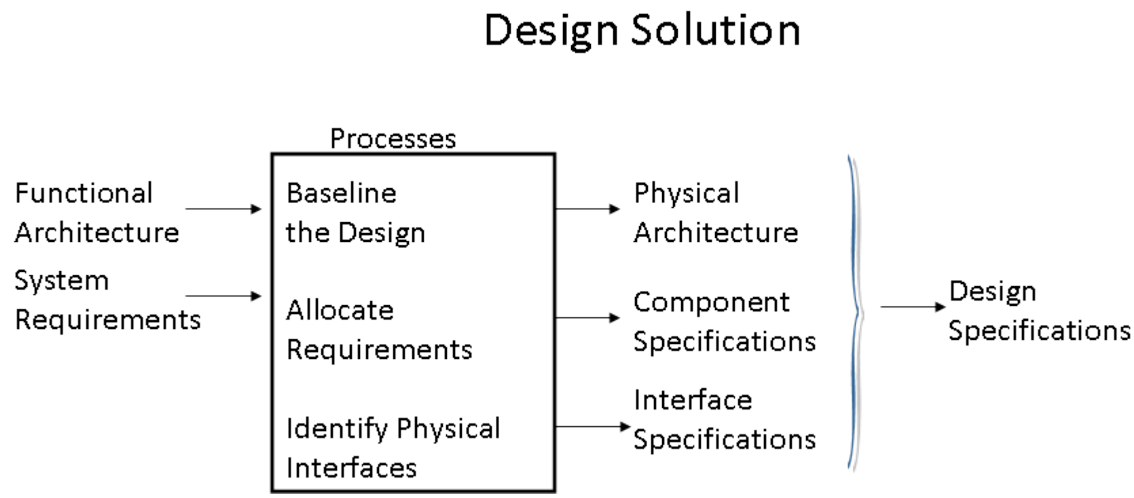


Figure 13-1. Input, Processes, Output Diagram

Essential Inputs

The primary input to the Design Solution process is the output of the Functional and Performance Allocation process, as follows:

- Functional Architecture
- System Requirements Document

Functional Architecture

The functional architecture is a hierarchical arrangement of functions and interfaces that represents the complete system, as described in the Functional & Performance Allocation chapter. The functions and sub-functions are arrayed in a functional architecture to show their relationships and internal and external interfaces. The resulting functional architecture may be represented in N^2 diagrams, IDEF0 diagrams, Functional Flow Block Diagrams, SV-4 diagrams, or any other functional diagram that illustrates the interaction of functions.

System Requirements Document

The System Requirements Document lists the complete set of system requirements, as described in the Functional & Performance Allocation chapter. Each system requirement is checked to establish that it is unique, complete, unambiguous, consistent with all other requirements, achievable (given current technologies or knowledge of technological advances), implementable, expressed at an appropriate level of detail, and verifiable. Deficiencies, conflicts, and weaknesses are identified and resolved within the complete set of system requirements (ISO-15288 2008).

Process Components

There are three main sub-processes needed to accomplish the Design Solution process:

- Baseline the Design
- Allocate Requirements
- Identify Physical Interfaces

The three sub-processes are iterative and may occur in parallel.

Baseline the Design

A set of alternative design solutions are generated, based on the functional architecture and requirements identified in the Functional & Performance Allocation process (IEEE 1220 2005). Required design characteristics (*e.g.*, color, texture, size, anthropomorphic limitations, weight, and buoyancy) are identified for the system under development. The systems engineer, along with the program office, identifies which design characteristics are constraints and which can be changed based on trade-off analyses (IEEE 1220 2005). Each alternative design solution is evaluated at a level of detail that permits comparison against the system requirements, including the performance, costs, time scales, and risks expressed in the stakeholder expectations (ISO-15288 2008).

The chosen design and performance characteristics are identified and documented. This design includes the estimation or measurement of physical and cognitive human-workload levels. The design characteristics and the human-engineering elements associated with life cycle quality factors must be identified and assessed. (IEEE 1220 2005).

The high-level activities performed during the Baseline the Design sub-process are as follows:

1) Determine which system requirements are allocated to human operators. This determination may involve "human-in-the-loop" scenarios and takes account of the context of use factors. At a minimum, it considers the following factors for the most effective, efficient, and reliable human-machine interaction:
   a) Limitations of human capabilities;
   b) Human actions critical to safety and how the consequences of error are addressed;

c) Integration of human performance into systems and their operation.

2) Determine whether hardware and software elements that satisfy the design and interface criteria are available, off-the-shelf. This determination includes evaluation of design elements that are not readily available, in order to determine if an element is to be developed, or if existing system elements will be re-used or adapted. Establish the costs, schedule, and technical risks associated with these make/modify/buy decisions.

3) Evaluate alternative design solutions, modeling them to a level of detail that permits comparison against the specifications expressed in the system requirements and the performance, costs, time scales, and risks expressed in the stakeholder requirements. This evaluation includes:

a) Assessing and communicating the emergence of adverse system properties resulting from the interaction of candidate system elements or from changes in a system element;

b) Ensuring that the constraints of enabling systems are taken into account in the design;

c) Performing effectiveness assessments, trade-off analyses and risk analyses that lead toward realizing a feasible, effective, stable, and optimized design.

The result of the sub-process is a documented, physical architecture representing the chosen system's design solution.

Allocate Requirements

Upon selection of a suitable physical architecture, the functions identified in Functional & Performance Allocation are partitioned and allocated to elements of the physical architecture in accordance with the system requirements (ISO-15288 2008). Common functions and sub-functions of the verified functional architecture are grouped into logical, functional elements in a manner that permits their allocation to design elements.

Allocation to design elements occurs when it is determined that the functional element can be accomplished by existing or newly developed items. If the functional element requires decomposition to permit its allocation, functional analysis is performed (see Functional & Performance Allocation) to partition the functional element sufficiently to permit its

allocation among hardware, software, and humans. Requirements traceability is established and recorded to ensure that all functions are allocated to elements of the system. Each system element performs at least one function (IEEE 1220 2005).

The selected physical design solution is specified in terms of its functions, performance, behavior, interfaces and unavoidable implementation constraints. These specifications are the actual system solution and an origin for system element acquisition agreements, including acceptance criteria. They may be in the form of top-level specifications, sketches, drawings or other descriptions appropriate to the maturity of the development effort, (e.g., feasibility design, conceptual design, pre-fabrication design, etc.). They are the criteria for deciding whether to produce, re-use or acquire system elements, for verifying the system elements and for defining an integration strategy for the system.

Identify Physical Interfaces

Although part of the physical architecture, physical interfaces between system elements and at the system boundary with external systems are defined and documented as interface specifications (ISO-15288 2008). Functional interfaces, captured in the functional architecture and system requirements, form the basis for physical interfaces. They are identified among products, subsystems, humans, life-cycle processes, and external interfaces to interacting systems. Design of physical interfaces may be impacted by communications, data, data rates, support, test, control, display, connectivity, and resource replenishment characteristics of the interfacing systems (IEEE 1220 2005).

The Interface Specifications Document captures the complete set of interface specifications for use in the implementation, integration, and verification processes. The documented interfaces are defined with a level of detail and control appropriate to the creation, use and evolution of the system entity and with interface documentation from parties responsible for external interfacing entities. Human-system and human-human interfaces are also defined and controlled (ISO-15288 2008).

Essential Outputs:

The primary output of the Design Solution process are the Design Specifications. The Design Specifications are composed of three parts:

- Physical Architecture
- Component Specifications
- Interface Specifications

Design Specifications

System, subsystem, and interface specifications that describe the specified requirements (system requirements and physical characteristics) are documented. This documentation records the structural and functional partitioning, the interface and control definitions, and the design decisions and conclusions, with traceability to the top-level system requirements baseline. Therefore, this document maintains mutual traceability with the system requirements.

The design baseline enables review in the event of change throughout the life cycle, as well as providing information for any subsequent re-use of the architecture. It is also the source from which tests during integration are conducted. Test criteria are determined to ensure that end products satisfy their specified requirements (EIA-632 1999).

The resulting design specifications denote the selected physical design solution as an architectural design baseline in terms of its functions, performance, behavior, interfaces, and unavoidable implementation constraints (ISO-15288 2008).

Although part of the Design Specifications document, descriptions of the specific outputs from each sub-process are as follows:

Physical Architecture Output

The physical architecture represents the design solution and physical interfaces. The physical architecture is used for requirements traceability and allocation matrices, which capture the allocation of functional and performance requirements among the system elements. Physical architecture definitions are documented, along with trade-off analysis results, design rationale, and key decisions to provide traceability of requirements up and down the architecture. Verification of the design architecture must be accomplished to demonstrate that the architecture satisfies both the validated requirements baseline and the verified functional architecture (IEEE 1220 2005).

Component Specifications Output

The system requirements and design constraints are transformed into appropriate component specifications in accordance with the identified physical architecture. The qualification section of individual specifications should identify the methods that will be used to confirm that each component specification has been satisfied under normal and abnormal conditions (IEEE 1220 2005).

Interface Specifications Output

The Interface Specifications denote the physical interfaces among products, subsystems, humans, life cycle processes, and external interfaces to interacting systems (IEEE 1220 2005). Within the FAA, the requirements associated with the interfaces are documented in Interface Requirements Documents (IRD) and the specifications to control the interfaces are documented in Interface Control Documents (ICD). See the Interface Management chapter 5 for more details on these documents.

Interdependencies

Interface Management
Integration
Verification
Risk Management
Configuration Management
Decision Analysis
Requirements Management

External Sources for More Detailed Information

Section 4.3 “Architecture Design Process” of the INCOSE Handbook (INCOSE 2010) depicts a similar process as the Design Solution process.

Readers interested in learning more on how to implement the systems engineering best practices represented in this chapter are referred to the following textbooks**:**

Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.

Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.

Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.

Sage, Andew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sage, Andew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Sobkiw, Walter. 2011. Systems Practices as Common Sense. Cherry Hill, NJ: CassBeth

References

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

14 – Implementation Process

Introduction

Implementation is the process that actually yields the lowest level system elements in the system hierarchy and gets the system element ready for the processes of integration. The Implementation process transforms specified functions, performance requirements, interfaces and implementation constraints, as documented in the design specifications, into a system element. Furthermore the implementation process should include some testing of the implemented system element before the element passes to the integration process. The systems engineer participates in the system element construction or adaptation by ensuring the appropriate plans and specifications are followed. The systems engineer also helps develop training for the system element, as appropriate. The process results in a system element that satisfies design specifications and stakeholder requirements through verification (ISO-15288 2008; INCOSE 2010).

Objective

The Implementation process realizes a specified system element (ISO-15288 2008).

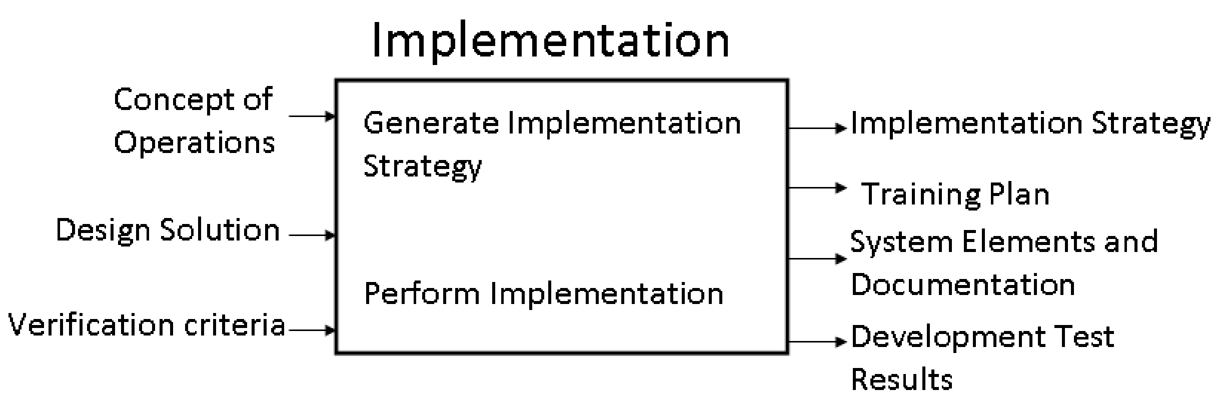


Figure 14-1. Input, Processes, Output Diagram

Inputs or Essential Criteria

The inputs to the Implementation process are created as the concept is designed. The essential criteria include verification criteria, which are listed on the "Vee diagram" after Implementation but are planned early in the life cycle.

Essential Inputs

Concept of Operations (CONOPS)

The CONOPS describes how a set of capabilities, from the user's perspective, will operate to enable operational improvements or achieve desired objectives for a proposed system. It describes the user organization(s), mission(s), and organizational objectives from an integrated system's point of view (IEEE 1362 1998). The document also describes any critical, top-level performance requirements or objectives, both stated either qualitatively or quantitatively. Finally, it describes system rationale as well as the roles, responsibilities, and skill sets needed for operations and maintenance of the implemented system (INCOSE 2010).

Design Specifications

The design specifications document describes the specified requirements (system requirements and physical characteristics) for the system, subsystems, and interfaces. This documentation records the structural and functional partitioning, the interface and control definitions, and the design decisions and conclusions, with traceability to the top-level system requirements baseline, and integration criteria is represented in the design. The design specifications document is the source where test criteria are determined to ensure that end products satisfy their specified requirements (EIA-632 1999).

Verification Criteria

Verification criteria include who will perform the verification during Implementation and the environment under which the verification is performed (INCOSE 2010). This criteria is developed and documented in the verification strategy during the Verification process

Process Components

Generate an Implementation Strategy

The implementation strategy includes implementation procedures, fabrication processes, tools and equipment, implementation tolerances, and verification uncertainties. It also includes a strategy for training the end users of the system. The implementation strategy document lists the constraints that the implementation strategy and implementation technology impose on the design solution. Additionally, it includes any current or anticipated limitations of the chosen implementation technology, contractor-furnished materials, or system elements for adaptation and it lists limitations resulting from the use of required implementation enabling systems (ISO-

15288 2008). This task produces the Implementation Plan and the Training Plan.

Perform Implementation

There are three main tasks for the systems engineer when performing the implementation. 1) The systems engineer oversee the building of system elements, 2) the systems engineer oversees or performs development testing, and 3) the systems engineer delivers or oversees the training of end users.

1) The systems engineer oversees the realization or adaptation of system elements using the implementation-enabling systems and specified materials according to the defined implementation procedures for hardware fabrication, software creation, and/or end-user training. Realization or adaptation is conducted with regard to standards that govern applicable safety, security, privacy, and environmental guidelines or legislation and the practices of the relevant implementation technology. The systems engineer records evidence that the built system element meets supplier agreements, legislation, and FAA policy (ISO-15288 2008). This effort may also involve packaging, handling, and storage, depending on where or when the system element needs to be integrated into a higher-level assembly. This task produces the system element and any supporting documentation.
2) The systems engineer performs development testing in accordance with the verification and testing plans to ensure the components are built according to the plans' requirements. This task produces some development test results.
3) The systems engineer delivers or oversees the appropriate supporting documentation and training to prepare end users for performing tasks in accordance with operational procedures and, as appropriate, confirms that the specified level of competence has been attained (ISO-15288 2008). The supporting documentation for the system element may include the manuals for operation, maintenance, and/or installation.

Essential Outputs

Implementation Strategy

The Implementation Strategy defines the general approach and success criteria for the system implementation. Each system element is identified in the strategy and any special cases are explained. The strategy identifies, in a Work Breakdown Structure, the activities expected during implementation,

and roles and responsibilities for the implementation are documented. The plan includes details on development testing and on any necessary end-user training. Finally, the strategy should address a means for feedback among the systems engineers, developers, and engineers responsible for building the system, and project managers. While overseeing the system build, the systems engineer needs a means to relay information and correct any problems.

Training Plan

The Training Plan is a detailed document of the training needs, priorities, and resources for end users of the implemented system. End users may include anyone who operates the system, maintains the system, or otherwise benefits from the system. The plan includes a description of how training is created, delivered, and evaluated for the implemented system.

System Element

A system element is packaged and stored in accordance with an agreement for its supply as documented in the Implementation Strategy Document. Although other engineers and developers build the system elements, systems engineering ensures the system elements are built in accordance with the plans and designs. The system elements include accompanying documentation such as the manuals for operation, maintenance, and/or installation The Implementation Plan provides guidance on the process to follow when discrepancies occur during the build.

Development Test Results

Documented results of the development test pertaining to the implemented systems element, as described in the Development Test Plan, Verification Plan, or Implementation Strategy Document.

Interdependencies

Technical Assessment
Validation
Verification
Risk Management

External Sources for More Detailed Information

The Implementation process is mostly an oversight effort by the systems engineer. Usually the actual implementation is performed by specific engineers and technicians. Therefore, more detailed information is specific to the task being performed, for the most part.

References

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association, January 7.

IEEE 1362. 1998. *IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document*. Standard. New York: The Institute of Electrical and Electronics Engineers, December 31.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

This page intentionally left blank.

15 – Integration Process

Introduction

In any systems engineering effort, there are system components (such as hardware items, software items, constituent systems within a system of systems, or the human systems that interact with the system) and there are process components (such as algorithms and system processes, operator processes, or business processes). Both sets of components must work together for the entire system to succeed.

The Integration process unifies the system components and the process components into a whole. It ensures that the hardware, software, and human system components will interact to achieve the system purpose and/or satisfy the customer's need. By principle, the integration process should improve performance, reliability, and/or interoperability without adversely affecting existing or proposed system functionality and operations. Integration can have a direct impact to internal/external interfaces as well as physical, logical and/or human-system interfaces while ensuring requirements and constraints are met (INCOSE 2010).

The purpose of the Integration Process is to assemble a system, regardless of complexity, that is consistent with the design specifications (ISO-15288 2008). Integration activities ensure that combining the lower-level elements results in a functioning and unified higher-level capability, with logical and design interfaces satisfied. Verification is conducted along with any integration activities. The integrated elements are tested to verify that the system meets system requirements. At each level of assembly and integration, the system entities should be subjected to sufficient testing to ensure operational effectiveness, usability, trainability, interface conformance, requirements conformance, ability to produce, and supportability (IEEE 1220 2005). However the Integration Process is not a *one-time event* and involves continuous, integrated, technical planning; monitoring; controlling; and assessing.

The Systems Engineering (SE) sub-processes in the Integration process are different than the other technical processes in that there is no dependency between them. Accordingly, only one sub-process is needed depending on the complexity of the system to be engineered. For traditional, albeit complicated, systems, system integration is followed. When a system is composed of multiple autonomous constituent systems, the appropriate sub-process is system-of-systems integration, which may differ from traditional systems integration.

The output of the process depends on whether the target is a system or a system of systems (SoS). An SoS differs from a complex system in that an SoS consists of multiple, diverse, autonomous systems, while the constituents of a complex system are not autonomous (Baldwin, Felder, and Sauser 2011). In other words, an SoS is composed of complex systems, which have all the qualities of a system in their own right. The output for system integration is a defined system integration strategy and an assembled and integrated system capable of being verified against the system and interface specifications from the design solution (ISO-15288 2008). For a SoS the output is only an integration strategy, albeit a potentially elaborate and complicated strategy. Since an SoS is assembled in part through evolution (Carlock and Fenton 2001; Maier 1998), no process can take full credit for its assembly. However, an integration strategy can encourage the assembly and evolution of an SoS.

Objective

The objective of the Integration Process is a functioning system or a plan to assemble a functioning system, regardless of complexity and in accordance with the design specifications.

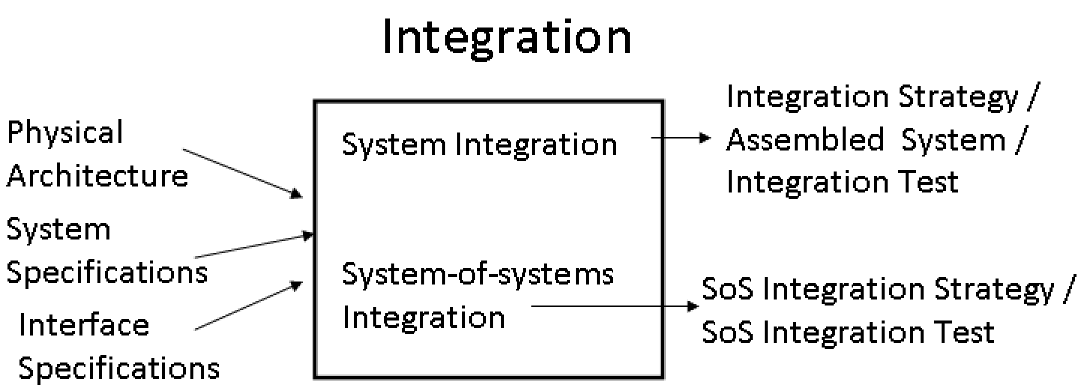


Figure 15-1. Input, Processes, Output Diagram

Inputs or Essential Criteria

Physical Architecture

The physical architecture represents the design solution and physical interfaces (IEEE 1220 2005). It is produced in the Design Solution process.

Interface Specifications

The Interface Specifications denote the physical interfaces among products, subsystems, parts, humans, life cycle processes, and external interfaces to interacting systems (IEEE 1220 2005). The interface specifications represent the physical and logical requirements that must be met by entities on both

sides of the interface, internal interfaces as well as external ones (Forsberg, Mooz, and Cotterman 2005).

System Specifications

Based on the system requirements and design constraints, subsystem and component specifications adhere with the identified physical architecture. These specifications identify the methods that will be used to confirm that each specification has been satisfied under normal and abnormal conditions (IEEE 1220 2005).

Process Components

There are two main sub-processes needed to accomplish the Integration process, as follows:

- System Integration
- System-of-Systems Integration

System Integration

The systems engineer must address any technology integration, business integration, and user integration. Technology integration can be defined as the melding of technologies into a uniform, functional working structure. Business integration refers to integration issues that arise when multiple organizations work together to complete a system. It can also refer to the integration of business processes. User integration addresses human factor issues and focuses on the system from an end-user point of view.

Integration activities are executed to ensure that combining the lower-level elements results in a functioning and unified higher-level element, with logical and design interfaces satisfied. The N^2 chart is one source of information for integration by illustrating relationships (and consequently interfaces) between elements (Forsberg, Mooz, and Cotterman 2005).

The project should progressively assemble and integrate subcomponents into complete components, components into assemblies, assemblies into subsystems, subsystems into products, and then (where meaningful) products and their life-cycle processes and services into a complete system. As system elements are assembled to form a complete component, new interface requirements will be generated and will need to be managed.

At each level of assembly and integration, the components, assemblies, subsystems, products, and system should be subjected to sufficient testing to ensure operational effectiveness, usability, trainability, interface conformance, ability to produce, supportability, and requirements conformance where applicable (IEEE 1220 2005). The interaction between

standards and interoperable components, such as COTS as a solution set, are the result of good integration also in accordance with systems engineering and software engineering best practices. An example of the different levels, different software modules can be integrated to form one software system; software and hardware systems can be integrated to form one computer system; and computer systems and business processes can be integrated to form one business system.

In the wake of integration, the systems engineer must stay mindful of existing legacy requirements, as well as new governance and logistical attributes, which may affect how the system is maintained or supported. The systems engineer should also stay in alignment with current standards and business processes. It is important to note that the system integration activities affect requirements management; the conceptual design; and various levels of architectures, testing, and production. Furthermore successful integration requires clear definition, documentation, and management of interfaces (Forsberg, Mooz, and Cotterman 2005).

Systems integration includes basic planning, preparation, execution, and integration testing. An integration plan is developed to define an assembly sequence and strategy that minimizes system integration time, costs, and risks, and to identify the constraints on the design arising. The preparation establishes the integration environment. Once the components are ready for assembly, integration is performed in accordance with applicable interface control descriptions and defined assembly procedures as defined in the integration plan (ISO-15288 2008). The system components are integrated with each other and with other interfacing systems. Integration tests are used to verify that the components and higher-level assemblies work together properly and do not interfere with one another (FHA 2007).

System-of-Systems Integration

There is much concern for system of systems integration in the Federal Aviation Administration as well as in the Department of Defense and other government agencies. However it is a poorly understood concept with sparse information in the academic literature. It appears that the development of a system of systems integration approach requires an understanding of system of systems (SoS).

First, the systems engineer must determine whether the system in question is an SoS or another classification of system (Baldwin, Felder, and Sauser 2011). Given that it is an SoS, different integration strategies may be required depending on the type.

A *virtual SoS* is generally unplanned when the component systems are engineered and acquired (Gideon, Dagli, and Miller 2005). A *collaborative*

SoS consists of component systems that willingly interact to fulfill the collective goal (Dahmann, Rebovich Jr, and Lane 2008). In both of these special cases, the SoS integration is relatively straightforward as the systems practically integrate themselves. Of course integration is much more complicated when a desired SoS is engineered.

On the other end of the spectrum is the *chaotic SoS*. This one has no agreed-upon goal and the constituent systems interact as they see fit. The random interactions cause unpredictable behavior (Gideon, Dagli, and Miller 2005). An *acknowledged SoS* has recognized overall goals but the constituent systems maintain their independence (Dahmann, Rebovich Jr, and Lane 2008). An example of this type of SoS is a federated system, where there is a central program office but the constituent systems participate via documented agreements.

More interesting from an integration standpoint, the *dedicated SoS* is built and integrated for a specific purpose (Dahmann, Rebovich Jr, and Lane 2008). They are consciously designed and engineered from the beginning to be an SoS (Gideon, Dagli, and Miller 2005).

Similar to systems integration, integration tests are used to verify that the constituent systems work together properly and do not interfere with one another.

Identifying the type of system based on its complexity and determining how each constituent system will impact the others are the first steps in SoS integration. However more detailed guidance is not yet available as system of systems integration is a burgeoning area with much research still needed.

Essential Outputs

Integration Strategy Plan / SoS Integration Strategy Plan

Since every system is unique, there is no one way to perform systems integration. There are three philosophies of integration: bottom-up, top-down, and big bang. The bottom-up approach is the classical method where components are connected one at a time. After each connection, the newly formed module is tested. Top-down integration assembles the top integrated modules and tests them. Then the branch of the module is tested step by step until the end of the related module. In the big bang approach, the developed components are coupled together to form a complete system or major part of the system and then tested (Ajaegbulemh 2010). An integration strategy should address the integration philosophy, the integration tasks, and details of the integration process.

The integration strategy defines the order in which the system components are integrated with each other and with other systems. Each integration step includes tests that verify the functionality of the integrated assembly, with particular focus on the interfaces (FHA 2007). There has to be careful planning so that the system is integrated in efficient, useful increments consistent with the system requirements and integrated technical plan.

According to (Forsberg, Mooz, and Cotterman 2005), an integration plan must address the following questions:

- Which integration tasks are needed?
- Who is responsible for each task?
- Where will the task be performed?
- What facilities and resources are needed?
- When will the integration take place?
- How will each integration task be verified (*i.e.*, against what requirements)?

Assembled System (System Integration)
Since a system of systems may take many years to build or evolve, the integration strategy plan is the primary output for SoS Integration. However for Systems Integration, the system can be assembled according to the plan during the allotted time. This assembled system adheres to the integration strategy plan and is capable of being verified against the system specifications, including the interface specifications, from the Design Solution process (see Chapter 13).

Integration Test
The integration test determines a successful integration has taken place by verifying the system or SoS against the functional, performance, reliability, and any other interface requirements. The result of integration testing is an integrated system or integrated SoS.

Interdependencies

Functional & Performance Allocation
Risk Management
Special Considerations for System of Systems
Integrated Technical Planning
Verification
Human Factors

External Sources for More Detailed Information

For more detailed description of system of systems, see (Baldwin, Felder, and Sauser 2011; Boardman and Sauser 2006; Boardman and Sauser 2008; Maier 1998). For more information on systems engineering an SoS, see (Carlock and Fenton 2001).

A more detailed discussion of integration as a bottom-up process and an alternate top-down integration process is presented in (Buede 2000, 305–311; Forsberg, Mooz, and Cotterman 2005, 361–366).

The FAA Test & Evaluation Handbook has more information related to integration testing (Air Traffic Organization, Nextgen and Operations Planning Services, Test and Evaluation Handbook, Document # VVSPT-A2-PDD-013 ver. 2.0, August 31, 2010)

References

Ajaegbulemh, Lakaisha. 2010. *The Integration of Roadmaps*. SDOE 605 Systems Integration Research Project. Hoboken, NJ: Stevens Institute of Technology, November 8.

Baldwin, W Clifton, Wilson N Felder, and Brian J Sauser. 2011. "Taxonomy of increasingly complex systems." *International Journal of Industrial and Systems Engineering* 9 (3): 298-316.

Boardman, John, and Brian Sauser. 2006. System of Systems - the meaning of of. In *Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering*, 118-123. Los Angeles, CA: IEEE, April. doi:10.1109/SYSOSE.2006.1652284.

———. 2008. *Systems thinking: Coping with 21st century problems*. Boca Raton, FL: CRC Press.

Buede, Dennis M. 2000. *The engineering design of systems: Models and methods*. New York: John Wiley & Sons.

Carlock, Paul G, and Robert E Fenton. 2001. "System of systems (SoS) enterprise systems engineering for information-intensive organizations." *Systems Engineering* 4 (4): 242-261.

Dahmann, Judith S, George Rebovich Jr, and Jo Ann Lane. 2008. "Systems engineering for capabilities." *CrossTalk: The Journal of Defense Software Engineering* 21 (November): 4-9.

FHA, Federal Highway Administration. 2007. *Systems Engineering for Intelligent Transportation Systems*. Washington, DC: US Department of Transportation, January.

Forsberg, Kevin, Hal Mooz, and Howard Cotterman. 2005. *Visualizing Project Management: Models and frameworks for mastering complex systems*. 3rd ed. Hoboken, NJ: John Wiley & Sons.

Gideon, James M, Cihan H Dagli, and Ann Miller. 2005. "Taxonomy of System-of-Systems." In *Proceedings CSER 2005*. Hoboken, NJ: Stevens Institute of Technology, March 23.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers, September 9.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering, January.

ISO-15288. 2008. *Systems engineering: System life cycle processes*. Standard. Geneva, Switzerland: International Organization for Standardization, February 1.

Maier, Mark W. 1998. “Architecting principles for system-of-systems.” *Systems Engineering* 1 (4): 267-284.

16 – Verification Process

Introduction

Despite the definitions, the most important aspect of validation and verification is that they are applied throughout the development and fielding of a system, but this manual adopts terminology with specific definitions outlined in this chapter and the Validation chapter.

The Verification process confirms that the system of interest and its elements meet the specified requirements. It determines the system is built as specified. The validated requirements are used for verification (INCOSE 2010). Verification ensures the requirements and specifications reflect the stakeholders' needs and trace accordingly (IEEE 1220 2005), and it ensures the selected system and subsystems meet their specified requirements (ISO-15288 2008; CMMI-DEV V1.2 2006).

This chapter covers the verification activities, where verification determines the system or service is built right, but not the details of performing verification.

The Systems Engineering (SE) activities in the Verification process are as follows:

1) Plan Verification
2) Verification Activities
    a. Verify Requirements/Specifications
    b. Verify Solution
    c. Verify Components
    d. Verify Subsystems and System
3) Identify Corrective Action

The primary outputs are the Verification Plan, which documents the strategy for performing verification, and the Verification Reports, which document the results of the verification activities and identify any corrective actions and results of re-verification. These documents may include or take the form of a Test and Evaluation Master Plan (TEMP) and a Verification Requirements Traceability Matrix (VRTM).

Objective

The verification process confirms that the specified design requirements are fulfilled by the system (ISO-15288 2008). In other words, that the system is built right, according to its specified requirements.

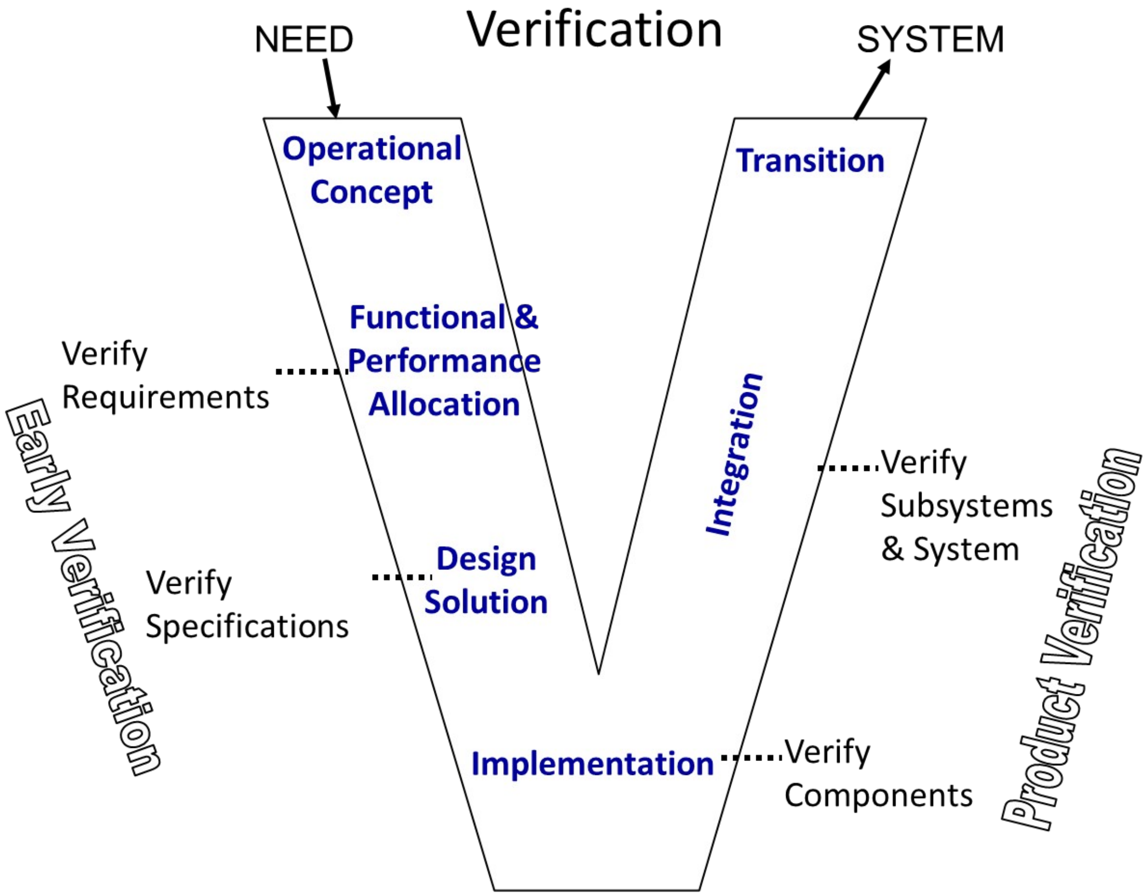


Figure 16-1. Systems Engineering “Vee” Diagram, Highlighting Verification

Verification Concepts

Verification includes the tasks, actions, and activities performed to evaluate the progress and effectiveness of the evolving system solution, via compliance with requirements. The basic verification activities are inspection, analysis, demonstration, and test. These activities may also apply, in some form, to validation. However, where validation is concerned with conforming to the stakeholders’ needs, verification activities are measured against the requirements.

Inspection

Inspection is performed by an examination of the system or component against applicable documentation to confirm compliance with requirements (INCOSE 2010).

Analysis

Analysis is the use of analytical data or simulations under defined conditions to show theoretical compliance of the system or component with requirements (INCOSE 2010).

Demonstration

Demonstration is a qualitative exhibition of functional performance of a system or component to show that a system or component responds to stimuli according to requirements (INCOSE 2010).

Test

Test, as used here, is an umbrella term to refer to any action by which the operability, supportability, or performance capability of an item is confirmed against requirements when subjected to controlled conditions that are real or simulated. Verification analysis checks that tests have been established using realistic scenarios to demonstrate human reaction times that satisfy operational requirements (INCOSE 2010).

There are four basic categories of test:

- **Development Test** – conducted on new items to demonstrate proof of concept or feasibility; known as DT at FAA
- **Operational Test** (OT) – includes OT and field familiarization; conducted to verify that the item meets its specification requirements when subjected to the actual operational environment
- **Qualification Test** – includes the production acceptance test (PAT) and the Independent Operational Assessment (IOA); conducted to prove that the system design meets its requirements with a predetermined margin above expected operating conditions
- **Acceptance Test** – known as SAT at FAA; conducted so that FAA can decide if the system is ready to change ownership from contractor to federal government (INCOSE 2010)

Although FAA may have more than four types of tests, each one falls into at least one of these basic categories. Furthermore, FAA may group different categories of test together, such as development and qualification tests into DT and some acceptance and operational tests into OT.

Plan Verification

During the earliest stages of the life cycle, a verification strategy is planned. In the FAA, this plan may take the form of a Test and Evaluation Master Plan (TEMP). The strategy of this plan applies to the system and to its descriptions, such as requirements and other systems engineering artifacts. The plan includes the context, purpose, nature, and scope for each verification action (ISO-15288 2008). The goal of the verification strategy is to ensure the system entity is built “right” (INCOSE 2010; ISO-15288 2008). The plan lays out a VRTM to ensure all specifications and requirements trace back to a validated need or operational scenario. Also the plan identifies the system and subsystem elements along with their verification method (demonstration, test, analysis, inspection), which may be included as part of the VRTM (IEEE 1220 2005). The plan must include some analysis to ensure any tests have been established using realistic scenarios to demonstrate human reaction times according to appropriate operational requirements. For more details on planning for verification, including the development of a TEMP, see the FAA AMS Lifecycle Verification and Validation Guidelines.

Verification Activities

Verification is a quality control process. Where variances are identified, they are recorded and guide corrective actions (ISO-15288 2008).

The activities of verification can be broken out as functional verification and design verification (IEEE 1220 2005), design solution verification and end product verification (EIA-632 1999), or just verification (INCOSE 2010; ISO-15288 2008). Also note IEEE-1220 and EIA-632 encompass traceability of requirements in verification, but ISO-15288 considers the traceability as part of the requirements development process. In this manual, the tracing of requirements to ensure they derive from the stakeholders’ need is early verification, and the act of documenting the traceability of requirements via a database is requirements management.

Verify Requirements

As requirements are decomposed and derived from the stakeholder expectations, the lower level requirements need to trace to the upper level, stakeholder expectations. Confirming this traceability is correct against other requirements or standards is known as requirements verification or functional verification (IEEE 1220 2005) and is covered in more detail in chapter 4 Requirements Management. However tracing requirements or specifications to ensure correctness is a form of validation.

Verify Specifications

As specifications are derived from system requirements, the lower level specifications need to trace to the upper level system requirements. Requirements validation determines whether requirements satisfy the defined quality criteria (e.g. correctness or completeness) in order to detect and correct any errors in the requirements as early as possible. Furthermore the design specifications must be verified against the base-lined system requirements. Also the system architecture is verified. The system architecture is composed of all physical architectures and life cycle process design architectures. Confirming this traceability is correct is known as specification verification or design verification (IEEE 1220 2005). Collectively tracing requirements or specifications to ensure correctness is a form of early verification.

Verify Components

Once system components are built during the Implementation process, they are verified against the approved specifications. This verification ensures the system components are built as expected. This activity is the first of the product verifications.

Verify Subsystems & System

As the components are integrated into a system, the expected functionality should emerge. To guarantee that this functionality is the correct functionality, the integrated subsystems and integrated system are verified against the appropriate system requirements. This activity is one of the product verifications. Also training material developed for the system is verified against the system requirements.

Identification of Corrective Action

As a result of verification, the system or a subsystem may be identified as non-conforming to one or many requirements. Verification data is collected, classified and collated according to criteria defined in the verification plan. This categorizes non-conformances according to their source and corrective action and owner. The verification data is analyzed to detect essential features such as trends and patterns of failure, evidence of design errors and emerging threats to services. The affected system or subsystem is isolated, and fault diagnosis is conducted to a level of resolution consistent with cost effective remedial action, including re-verification following defect correction (ISO-15288 2008).

Essential Outputs

Verification Plan

The verification plan should include, at a minimum, the work products, such as the system or components, to be verified (CMMI-DEV V1.2 2006); the selection and definition of the appropriate method for verification; verification procedures to be followed for the method selected; the purpose and objective of each procedure, pretest action, and post-test action; and the criteria for determining the success or failure of the procedure (EIA-632 1999). This plan may be developed in the form of a TEMP and should include a VRTM. For more information on the TEMP and VRTM in the FAA, see the FAA AMS Lifecycle Verification and Validation Guidelines.

Verification Report

Verification data are the results of the various verification activities and are documented in verification reports, including updates to the VRTM. When verification issues are identified, the activity, results of the activity, recommendation for corrective actions, and any other relevant data are documented in the report. Otherwise objective evidence that the realized product satisfies the system requirements and the design solution is provided (ISO-15288 2008).

This report is updated after the actions have been taken along with the results based on the corrective actions. For details on the verification reports, see the FAA AMS Life Cycle Verification and Validation Guidelines.

Interdependencies

Validation
Requirements Management

External Sources for More Detailed Information

V&V Working Group
Test Standards Board
V&V Guidelines

References

CMMI-DEV V1.2. 2006. *CMMI for Development, Version 1.2*. Standard. Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization.

This page intentionally left blank.

17 – Validation Process

Introduction

This manual adopts a consistent definition for Validation, which adheres to systems engineering standards (CMMI-DEV V1.2 2006; EIA-632 1999; IEEE 1220 2005; INCOSE 2010; ISO-15288 2008). In the end, the most important aspect is that validation and verification are applied throughout the development and fielding of a system.

The Validation process confirms the completed system satisfies or will satisfy the stakeholders' needs. It determines if a system does everything it should do and nothing it should not do. Stakeholders and end-users, or their validated documented expectations, are involved in validation (INCOSE 2010). In all cases, system validation is ratified by stakeholders (ISO-15288 2008).

Validation demonstrates whether a product will fulfill its specified purpose when placed in its intended environment (CMMI-DEV V1.2 2006) and may be applied to documentation, products, or both. Validation of documents ensures the written expectation, requirement, or specification represents the users' needs, while validation of products ensures an operationally effective and suitable end product (FAA 2012).

This chapter covers the validation activities but not how to perform the validation. This difference is important since validation is ratified by stakeholders, but its implementation may involve a representative of the stakeholder. For example, the stakeholder may witness a demonstration of the system. The stakeholder may validate the design of a user interface in a rapid prototyping environment. The system components may be validated with use cases developed jointly with the stakeholder.

The Systems Engineering (SE) activities in the Validation process are as follows:

1) Plan Validation
2) Perform Validation
    a. Validate Need
    b. Validate Operational Scenarios
    c. Validate Requirements
    d. Validate Solution
    e. Validate System

f. Validate Operations

The primary outputs are the Validation Plan, which documents the strategy for performing validation, and the Validation Report, which documents the results of the validation activities.

Objective

The Validation process provides objective evidence that the right system is built and achieves its intended use in its intended environment by involving the appropriate stakeholders as often as possible.

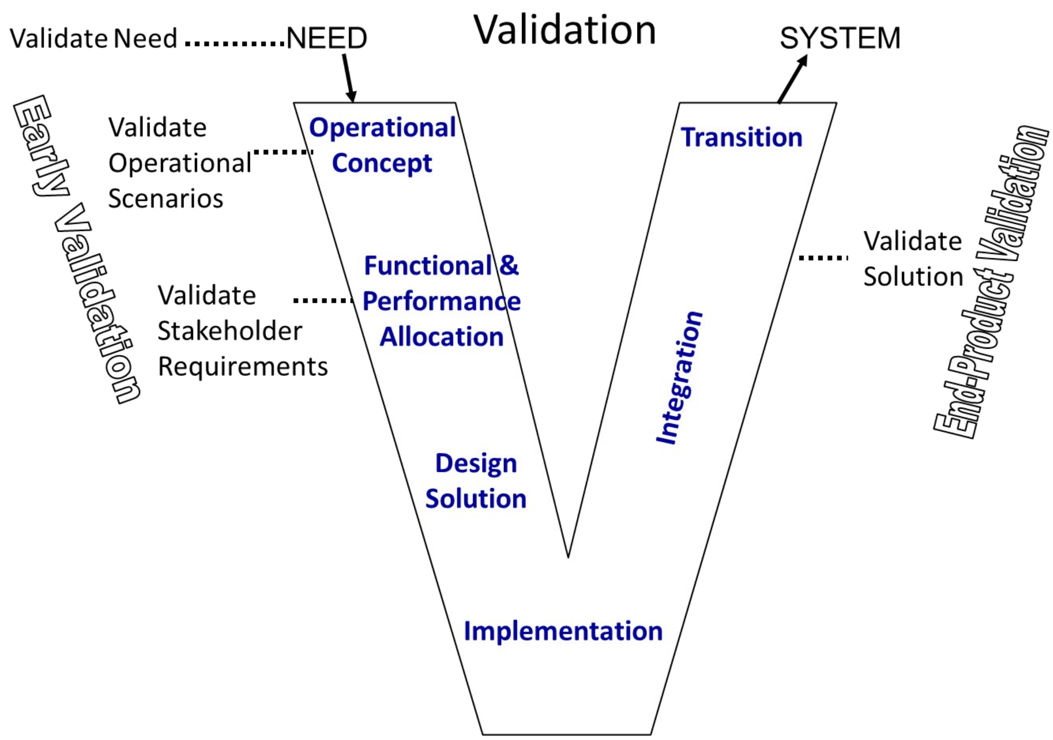


Figure 17-1. Systems Engineering “Vee” Diagram, Highlighting Validation

Plan Validation

Validation strategies are planned during the earliest stages of the system’s life cycle. This plan documents the strategy to demonstrate, via assessment of the services presented to the stakeholders, that the system is fit for its purpose and satisfies the end user (ISO-15288 2008). The goal of the validation strategy is to ensure the "right" system entity has been created. Although validation ensures the representation of stakeholder expectations,

validation in some phases of the life cycle may be based on the validated requirements baseline (IEEE 1220 2005).

Validation Activities

Validation is a process for the benefit of the stakeholders. Stakeholders can be an enterprise, organization, or an individual, such as the end users, having an interest or a stake in the outcome of the engineering of a system (EIA-632 1999). Validation performs a comparative assessment to demonstrate a system is fit for its purpose and satisfies the stakeholder. Where variances are identified, they are recorded and guide corrective actions (ISO-15288 2008).

The activities of validation can be broken down into requirements validation and end-product validation (EIA-632 1999) or simply consolidated as validation (INCOSE 2010; ISO-15288 2008). In any case, the following validation activities are performed, regardless of their names.

Validate Need

Problem statements representing the agency needs, goals, or shortfalls are formally defined the Operational Concept process. Within FAA, the Capabilities, Gaps, and Opportunities statement may describe these problem statements. In any case, these needs are validated with the stakeholders.

Validate Operational Scenarios

Operational scenarios and stakeholder expectations represent the initial requirements for a system or capability. These scenarios must be validated to ensure they represent the stakeholders' needs and to determine whether the full spectrum of possible system operations and system life cycle support concepts have been adequately addressed (IEEE 1220 2005). These early design artifacts may represent the stakeholders' interests for the purpose of validating detailed requirements and designs.

Validate Stakeholder Requirements

Every requirement, regardless of its form or name, must be validated to ensure it represents identified stakeholder expectations and project, enterprise, and external constraints and to determine whether the full spectrum of possible system operations and system life cycle support concepts has been adequately addressed (IEEE 1220 2005). Validation may take the form of peer reviews, walkthroughs, simulations, or analysis, although this list is not inclusive. The requirements statements may be validated against the validated designs, such as the operational scenarios or stakeholder expectations, or possibly validated with the end-users using a walk-through of the functional architecture. Tracing requirements is covered in more detail in Chapter 4: Requirements Management.

Validate Solution

When a physical architecture is selected, the solution is validated. This validation is usually against validated designs but the stakeholders may be directly included, if reasonable. The validation may include demonstrations, audits, analysis, or checklists.

Validate System

As the components are integrated into a system, the expected functions should emerge. To guarantee that this functionality is the correct functionality, the system is validated with the stakeholders. Training material developed for the system is validated also with the end user and any other stakeholder that may need to be trained on the system. The system validation may include tests, demonstrations, audits, analysis, or checklists. Validation of the training material could be performed via peer reviews, walkthroughs, or trial by user.

Validate Operations

As the system is integrated into the NAS, its final functionality emerges. To guarantee the system accomplishes its objectives, it is validated with the actual stakeholders and end-users.

Essential Outputs

Validation Plan

The validation plan should include, at a minimum, the products to be validated, the environment to conduct the validation, and the specific validation procedures and criteria (CMMI-DEV V1.2 2006). Validation should be accomplished using the actual artifact operating in its intended environment or as close a facsimile of the environment as possible.

Validation Report

The Validation Report is the documented validation data of results from the various validation activities. When validation issues are identified, the activity, results of the activity, and recommendation for corrective actions are documented in the validation report. This report is updated after the actions have been taken along with the results based on the corrective actions. The validation reports are an important input to the decision milestones throughout the system life cycle (INCOSE 2010).

Interdependencies

Verification
Risk Management

External Sources for More Detailed Information

V&V Working Group
Test Standards Board
V&V Guidelines (FAA 2012)

References

CMMI-DEV V1.2. 2006. *CMMI for Development, Version 1.2*. Standard. Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute.

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association.

FAA, Federal Aviation Administration. 2012. *FAA AMS Life Cycle Verification and Validation Guidelines, Ver 2.0*. Atlantic City International Airport, NJ: William J Hughes Technical Center.

IEEE 1220. 2005. *IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering.

IREB. 2012. “International Requirements Engineering Board.” http://www.certified-re.de/en/.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization.

This page intentionally left blank.

18 – Deployment and Transition

Introduction

The Deployment and Transition phase both encompass a variety of preplanning, assessment, and preparation activities which are essential to a system before it can be fielded; these activities help determine the readiness of a solution being implemented and ensure that the system-of-interest will maintain integrity and resilience while in-service. Trouble-free deployment and transition requires thorough planning early in the lifecycle and collaborative efforts between the service organization(s), facility team(s), system contractor(s), and regional and site personnel.

Deployment planning is part of a continuous In-Service Review process that begins early in the lifecycle management process, usually during development of requirements in the Concept and Requirements Development portion of the AMS Mission Analysis phase.

Transition involves all work activities for installing the new system at the key site, conducting the tests for reaching the In-Service Decision (ISD), and transitioning from the legacy to the new system. It also covers all work activities to install subsequent systems at each operational site and qualify them for operational service. This includes the transition planning section of the Life Cycle Plan (see Chapter 27: Life Cycle Engineering), which documents how to transition operations and maintenance from the existing system to the new system. The scope of activities includes preparing the site, installing and testing the equipment, conducting dual operations, familiarizing field personnel with the new equipment, obtaining full operational support, and removing and disposing of replaced assets. Transition occurs following the AMS Solution Implementation Phase and prior to the AMS In-Service Management phase. Ultimately, the Transition Process transfers custody of the system and responsibility for system support from one organizational entity to another. This includes, but is not limited to, transfer of custody from the development team to the organizations that will subsequently operate and support the system. Successful conclusion of the Transition Process typically marks the beginning of the In-Service Management Phase of the system-of-interest.[1]

[1] INCOSE Systems Engineering Handbook v. 3.2, January 2010, p. 130

Objective

Deployment

The underlying objective is to ensure that all operational aspects have been accounted for prior to transitioning to a new system, capability, or functionality. All programs undergo some degree of deployment planning and assessment to ensure that key aspects of fielding a new capability are thoroughly planned and implemented; in addition, it should also ensure that deployment does not create a critical deficiency or adverse effect to the system of interest.

Transition

From an operational standpoint, the clear objective is to facilitate a seamless “hand-off” or switchover to the new system-of-interest, functionality, or capability. In the case where legacy constraints are preeminent or expected to be phased out or replaced, the ultimate goal is to incur minimum to zero risk to the existing or future operational state.

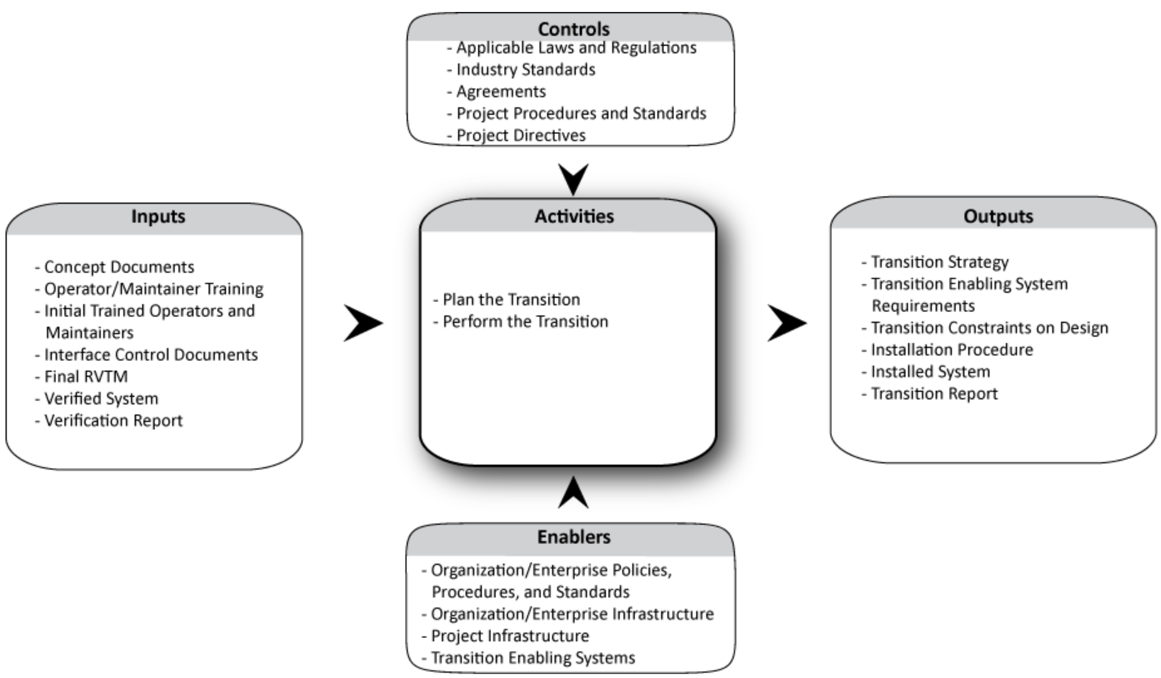


Figure 18-1. Context Diagram for the Transition Process

Deployment and Transition Inputs

The inputs for the Deployment and Transition process include:

- Implementation schedule (identifies when each site will receive the new equipment and dispose of the old)
- Test schedule (used in developing the overall deployment and implementation schedule)
- FAA/ATO policy (will identify the steps for deployment and commissioning)
- Concept Documents
- Operator/Maintainer related Documents and Training
- Initial Trained Operators and Maintainers
- Interface Control Documents
- Final RVTM
- Verified System
- Verification Report

Deployment and Transition Process

Deployment planning involves coordination among and participation by many critical functional disciplines. Tradeoffs among cost, schedule, performance, and benefits relative to these functional disciplines must also include the impact of deployment and implementation considerations. Deployment planning tools (such as a tailored In-Service Review Checklist) assist in identifying, documenting, and resolving deployment and implementation issues.

Methods and techniques include, but are not limited to, a tailored application of generic tools; integration of checklist issues with other emerging issues (such as problem test reports from test and evaluation); development of action plans to resolve checklists and other items; and documentation of issue resolution and mitigation results. Consistent deployment planning shall be documented in the contractor’s Statement of Work and associated efforts. The results of deployment planning (and issue resolution) are briefed periodically (e.g., at acquisition reviews), presented at the ISD meeting, summarized in an ISD memorandum, and audited during the post-ISD follow-up and monitoring activities.

Deployment and Transition Activities

The Transition Process includes the following activities:[2]

- Plan the Transition
  - Prepare a transition strategy, including operator training, logistics support, delivery strategy, and problem rectification/resolution strategy.
  - Develop a cutover plan for key site
  - Develop installation procedures

- Perform the Transition
  - Prepare key site for new system per established procedures
  - Install and check out system at key site per established procedures
  - Train the users in the proper use of the system and affirm users have the knowledge and skill levels necessary to perform Operation and Maintenance activities. This includes a complete review and handoff of operator and maintenance manuals, as applicable.
  - Integrate and verify system at key site
  - Prepare Independent Operational Test Readiness Declaration
  - Conduct Independent Operational Test and Evaluation
  - Conduct field familiarization testing for key site
  - Receive final confirmation that the system—as operated and maintained by the intended users—meets the users' needs. This process typically ends with a formal, written acknowledgement that the system has been properly installed and verified, that all issues and action items have been resolved, and that all agreements pertaining to development and delivery of a fully supportable system have been fully satisfied or adjudicated
  - Prepare for the ISD
  - Obtain the ISD
  - Conduct dual operations at key site
  - Commission key site into operational service

[2] INCOSE Systems Engineering Handbook v. 3.2, January 2010, p. 132

- Document Post-implementation problems; they may lead to corrective actions or changes to the requirements
- Dispose of replaced assets at key site
- Develop cutover plan for each site
- Prepare each site for new system
- Install and check out system for each site
- Integrate and test system for each site
- Conduct field familiarization testing for each site
- Conduct dual operations for each site
- Commission in operational service for each site
- Dispose of replaced assets for each site

Common Approaches and Tips

When acceptance activities cannot be conducted within the operational environment, a representative locale is selected. The Deployment and Transition process relies heavily on quality assurance (QA) and configuration management documentation.

This process is governed by the following controls and enablers:

- Applicable Laws and Regulations
- Industry Standards – relevant industry specifications and standards
- Agreements – terms and conditions of the agreements
- Project Procedures and Standards – including project plans
- Project Directives
- Organization/Enterprise Policies, Procedures, and Standards – including guidelines and reporting mechanisms
- Organization/Enterprise Infrastructure
- Project Infrastructure
- Transition Enabling Systems – examples include storage, shipping, and training

Deployment and Transition Outputs

Completion of an In-Service Review Checklist and an ISD allows the system to be deployed to the field, marking the entrance to the In-Service Management phase of AMS.

The final output of deployment and transition is a commissioned system and the disposal of the old system. Other outputs include:

- Transition Strategy
- Transition Enabling System Requirements – Requirements for any system needed to enable transition of the system-of-interest need to be developed
- Transition Constraints on Design – Any constraints on the design arising from the transition strategy
- Installation Procedure
- Transition Report – Including documentation of the transition results and a record of any recommended corrective actions, such as limitations, concessions, and on-going issues. The transition report should also include plans to rectify any problems that arise during transition.

Interdependencies

Configuration Management
Validation
Verification
Life Cycle Engineering

References

EIA-632. 1999. *Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association.

INCOSE. 2010. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering.

ISO-15288. 2008. *Systems Engineering: System Life Cycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization.

19 – Service-Gap Analysis

Introduction

Service-gap analysis is the first phase in the AMS life cycle; it relates to Systems Engineering in the Operational Concept process. Service-gap analysis is conducted in response to a priority service need within an EA Roadmap that is vital to FAA accomplishing its overall mission.

Acquisition Management System

The Acquisition Management System (AMS) establishes policy and guidance for all aspects of life cycle acquisition management for the Federal Aviation Administration (FAA). It defines how the agency manages its resources (money, people, and assets) to fulfill its mission. The objectives of the policy are to increase the quality, reduce the time, manage the risk, and minimize the cost of delivering safe and secure services to the aviation community and flying public. Acquisition management policy promotes these objectives through partnership among service providers and customers to ensure FAA plans, programs, and budgets address priority aviation needs.

FAA developed the Acquisition Management System in response to Section 348 of Public Law 104-50. The AMS supersedes the Major Acquisition Policies and Procedures of the Department of Transportation and all other acquisition and procurement statutes and regulations, including the Federal Acquisition Regulation. AMS policy takes precedence over all other FAA policy dealing with any aspect of lifecycle acquisition management and related disciplines.

National Airspace System

The National Airspace System (NAS) is a highly complex system of systems. There are numerous facilities, structures, and pieces of equipment that together form the safest and most efficient aerospace system in the world. Advances in technology, increased demand, obsolescence of existing systems, and an evolving group of stakeholders signify that the aviation landscape is changing. Within this changing landscape, FAA must carefully plan to sustain the current infrastructure while transitioning to the NAS of the future.

FAA Corporate Investment Strategy Development Process

Figure 19-1 illustrates how the agency determines where and when it will invest. Corporate strategic planning consists of processes that update the Enterprise Architecture and its roadmaps and Destination 2025 (formerly known as the FAA Flight Plan) each year. The EA roadmaps specify when priority service needs or shortfalls enter the AMS Life Cycle management

process for resolution. Destination 2025 establishes strategic and performance goals for the agency over the next 15 years.

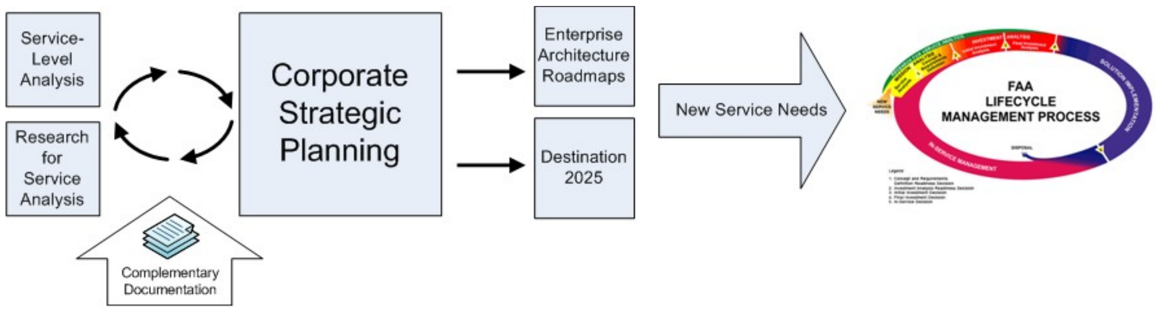


Figure 19-1. FAA Corporate Investment Strategy Development Process

Inputs

Service-level analysis and research for service analysis are key inputs to corporate strategic planning.

Service-level analysis is conducted by service organizations to determine which future investments are needed to sustain, improve, and modernize the NAS and other auxiliary FAA services. During this analysis, service organizations analyze current performance, sustainability, and obsolescence of operational assets along with projected needs for services. This analysis results in a prioritization of required investments and an investment timeline for each service organization.

Research for service analysis consists of research, engineering & development (R,E&D) and concept maturity and technology development (CMTD). R,E&D is a research, engineering, and development portfolio that studies new concepts, products, and procedures with potential benefits for the aviation community. Goals, activities, and accomplishments are published annually in the National Aviation Research Plan (NARP). CMTD undertakes feasibility studies, prototype demonstrations, and technical analyses that evaluate and mature potential concepts for improving service delivery.

Both service-level analysis and research for service analysis have an iterative relationship with corporate strategic planning. Corporate strategic planning is an enterprise-level management process that integrates the investment needs of each service organization and associated infrastructure improvements with investments necessary to transition to the next generation air traffic control system. There is an ongoing dialogue between management and service organizations during the strategic planning process that results in continual adjustments and iterations to ensure a feasible and

realistic strategy is sustained over time. This dialogue includes considerations for any additional factors that may impact the investment strategy for the agency. These factors may be contained in complementary documents that include: the Joint Planning and Development Office Concept of Operations, NextGen Implementation Plan, and the RTCA NextGen Mid-Term Implementation Task Force Report.

The final plan and strategy for implementation is documented in the Enterprise Architecture roadmaps and Destination 2025. The Enterprise Architecture develops and maintains enterprise architecture views, reconciles, and approves segment architecture for the agency's core lines of business. The EA Roadmaps specify when investment opportunities should enter the AMS Life Cycle and highlight interdependencies between investments. Destination 2025 defines specific performance goals and measures for the agency. Together, these outputs describe FAA's plan to satisfy its legislative mission.

AMS Phase Structure

In the section that follows, each AMS phase activity is described along with the specific responsibility of the systems engineer using the following structure:

- **A phase diagram** that illustrates and encapsulates relationships among phase entrance criteria, inputs, activities, outputs, and the systems engineering role.
- **Phase activity descriptions** that include activity inputs, outputs, and the systems engineering role. The systems engineering role is a generic role that may be filled by different individuals as a service need travels the AMS Life Cycle management process to resolution. Even within a specific life cycle management phase activity, the assigned systems engineer may engage assistance from other engineering resources to complete the work.
- **Useful references and tools** that may assist completion of phase activities.

Service-Gap Analysis Process

Service-gap analysis develops a qualitative preliminary description of the priority need, existing legacy assets, capability shortfall, and develops the Concept and Requirements Definition Plan. This activity ends with a Concept and Requirements Definition Readiness Decision, which marks official transition from service-gap analysis to concept and requirements definition. Service-gap analysis may also be conducted for important service needs not within an EA roadmap as the basis for determining whether to add them.

SERVICE-GAP ANALYSIS DIAGRAM

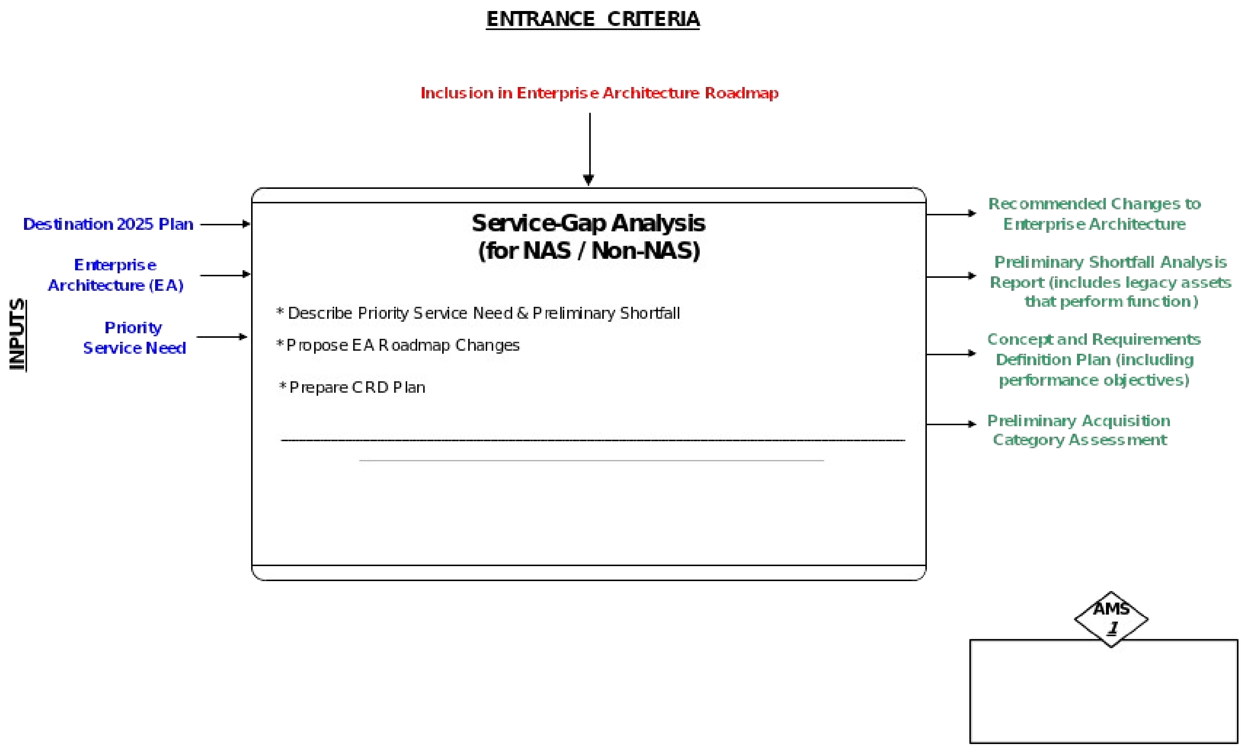


Figure 19-2. Service-Gap Analysis Systems Engineering Inputs and Outputs

Service-Gap Analysis Activities

The activities in this process include the following:

- Describe Priority Need and Preliminary Shortfall
- Propose EA Roadmap Changes
- Prepare CRD Plan

These activities are described below.

Describe Priority Need and Preliminary Shortfall

When an EA roadmap specifies a new service need is an agency priority, the responsible service organization defines the capability that must be put in place to improve service delivery and achieve agency strategic and performance goals. The service organization also describes legacy assets or existing systems, facilities, people, and processes that now perform the function or service. With this information, the service organization defines the service shortfall and the difference between future service need and current capability as a foundation for understanding the problem and its nature, urgency, and impact. The service need, shortfall, and legacy case are documented in the Preliminary Shortfall Analysis Report.

Systems Engineering Role
The systems engineer takes the lead in describing the preliminary service need and legacy assets. The systems engineer is also responsible for defining the infrastructure shortfall.

Activity Inputs
Destination 2025
Enterprise Architecture Roadmap
Priority Service Need

Activity Output
Preliminary Shortfall Analysis Report, including a description of legacy assets currently performing the function

Potential SEM Chapter Reference
Operational Concept

Propose Enterprise Architecture Roadmap Changes
For important, new, service needs not contained in an EA roadmap, the service organization prepares the products and amendments necessary to propose a change to the Enterprise Architecture or its roadmaps. Approval is required before entry into concept and requirements definition.

Systems Engineering Role
The systems engineer supports development of solution-level architectural products necessary to support EA roadmap changes.

Activity Inputs
Destination 2025
Enterprise Architecture
Priority Service Need

Activity Outputs
Specific recommended changes to an Enterprise Architecture Roadmap

Potential SEM Chapter References
Specialty Engineering
Technical Data Management
Interface Management

Prepare Concept and Requirements Definition (CRD) Plan
The CRD Plan specifies the tasks of Concept and Requirements Definition and how they will be accomplished, defines the roles and responsibilities of participating organizations, defines outputs and exit criteria, establishes a schedule for completion, and specifies needed resources. ATO Systems

Engineering and Safety works with the responsible service organizations to assist in the preparation of this plan. Organizations that sign onto the CRD Plan agree to provide the necessary resources.

Systems Engineering Role
The systems engineer ensures sufficient engineering resources and time are included in the CRD Plan to complete the activities of concept and requirements definition.

Activity Inputs
Concept and Requirements Definition Plan template and instruction

Activity Outputs
Concept and Requirements Definition Plan

Potential SEM Chapter References
None

Other Systems Engineering Responsibilities During Service-Gap Analysis

Integrated Technical Planning executed in service-gap analysis is the strategic means of defining problems, forecasting conditions, and coordinating solution elements to provide superior outputs, inputs to the next phase of the life cycle.

Interdependencies

Risk Management
Configuration Management
Technical Assessment
Decision Analysis
Operational Concepts

References and Tools

Reference	Description
Joint Planning and Development Office (JPDO) *Concept of Operations* http://www.jpdo.gov/library/NextGen_v2.0.pdf	The JPDO CONOPS provides an operational view of NextGen and how it will operate in 2025 and beyond. It includes the role of every air transportation stakeholder (NASA, DoD, DOT, DHS, etc). This document should be used as a reference to understand the long-term impact of capabilities on the overall management of air traffic.
Radio Technical Commission for Aeronautics (RTCA) *NextGen Mid-Term Implementation Task Force Report* http://www.faa.gov/about/initiatives/nextgen/media/nextgen_progress_report.pdf	The RTCA task force report was created to forge community-wide consensus on the recommended NextGen operational improvements to be implemented during the transition between now and 2018. The task force looked for opportunities to accelerate the transition to technologies defined in the NextGen implementation plan. This document should be used as a reference to understand the specific strategies for accelerating certain types of technology.
Federal Aviation Administration (2010) *National Aviation Research Plan* http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/nextgen/research_tech_dev/research_planning/narp/media/pdf/NARP_2010.pdf	The NARP establishes the research and development programs for FAA. Published annually, the NARP bridges the near-term goals of the FAA Flight Plan (2009-2013) with the mid-term goals of the NextGen Implementation Plan (2012-2018) and the far-term goals of the JPDO's Integrated Work Plan (2015-2025). The NARP can be used to understand the impact a specific technology has on the goals of the agency in the near, mid, and far term.

Reference	Description
Federal Aviation Administration (2010) *NextGen Implementation Plan* https://intranet.faa.gov/faaemployees/org/linebusiness/ato/operations/technical_operations/ajw1/ajw14/media/NextGen%20Implementation%20Plan%202010.pdf	The NextGen Implementation Plan provides an overview of the FAA's ongoing transition to NextGen. The plan lays out the agency's vision between now and the mid-term time frame (2012-2018). The plan identifies the goals for technology and program deployment. This document should be used to tie specific program shortfalls to the goals of NextGen.
Federal Aviation Administration (2009-2013) *FAA Flight Plan* (to be replaced by FAA Destination 2025) http://www.faa.gov/about/plans_reports/media/flight_plan_2009-2013.pdf	The Flight Plan contains the five-year strategic plan for FAA from 2009 through 2013. FAA is currently developing a replacement for the Flight Plan called "Destination 2025." This document should be used to tie specific program shortfalls to the strategic goals of the agency. There should be a direct link between a strategic goal for improvement and the shortfall identified during service-level analysis.
Federal Aviation Administration (2010) *Investment Decision Authority (IDA) Process Guidance* https://intranet.faa.gov/faaemployees/org/linebusiness/ato/acquisition_business/ipm/media/file/Preparing%20for%20a%20JRC/IDAGuidance%208_13_2010.pdf	This document is supplemental to the information in AMS policy. It explains the types of decisions and prerequisite actions, roles and responsibilities, and procedures required to receive an investment decision from an agency investment decision authority. This document should be used to reference all items that must be completed prior to a Concept and Requirements Definition (CRD) Readiness Decision.

Reference	Description
Federal Aviation Administration. (2011) *Acquisition Management System Policy* http://fasteditapp.faa.gov/ams/do_action?do_action=ListTOC&contentUID=4	AMS Policy establishes all requirements for acquisition management at FAA. Specifically, it contains service analysis and CRD requirements for the activities that must be completed, the outputs and products of each activity, who is responsible for each activity, and who approves each output.
Federal Aviation Administration (2006) *National Airspace System, System Engineering Manual* (Version 3.1) http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/sysengsaf/seman/	This previous version of the NAS systems engineering manual provides a framework for implementing systems engineering across FAA. The document does not mandate any formal practice but acts as a reference for conducting specific systems engineering activities.
Federal Aviation Administration (2007) *National Airspace System Enterprise Architecture Framework (NASEAF), Volume III: Product Implementation Methodologies* (Version 2.00) https://nasea.faa.gov/file/get/814	This document describes the Air Traffic Organization’s method for building architectures. It defines and describes the products and processes that apply to architecture development for all levels (enterprise, service-unit, and project). This document can be used to understand the NAS EA framework and its structure. It should be referenced during the construction of project-level architecture products and amendments.
Federal Aviation Administration (2010) *Service Analysis and Concept and Requirements Definition Guidelines*, (Version 4.0) http://fast.faa.gov/mission/conc_req_def.htm	This document describes “how-to” guidance for moving through the service analysis and CRD phases of AMS. The document includes specific information such as templates, process instructions, required reviewing organizations, and required signature authorities. This document in addition to AMS policy should be used to understand the AMS requirements for service analysis and CRD.

This page intentionally left blank.

20 – Concept and Requirements Definition

Introduction

Concept and Requirements Definition is the second phase within the AMS life cycle. Operational Concept is furthered and the Functional and Performance Allocation systems engineering function is initiated in this phase.

Concept and requirements definition has two primary goals:

- Translate priority service needs in an Enterprise Architecture roadmap into preliminary requirements and a Solution Concept of Operations (CONOPS)
- Identify and define the most promising alternative solutions deemed best able to satisfy the priority service need efficiently and effectively

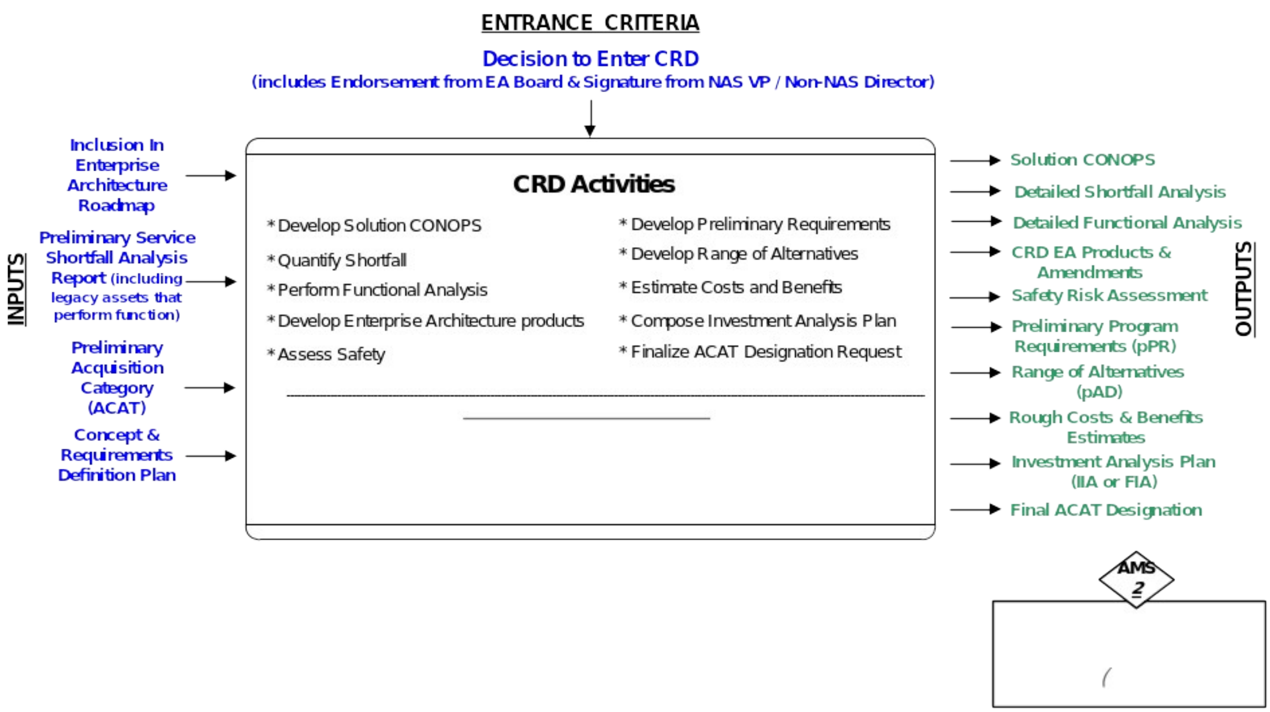


Figure 20-1. CRD Activities, Inputs, and Outputs

CRD Activities

The activities in this process include the following:

- Develop Solution CONOPS
- Quantity Shortfall
- Perform Functional Analysis
- Develop EA Products

- Assess Safety Risk
- Develop Preliminary Requirements
- Develop Range of Alternatives
- Estimate Cost and Benefits
- Compose IA Plan
- Finalize ACAT Designation Request

These activities are described below.

Develop Solution Concept of Operations

The Solution CONOPS describes the functional and operational characteristics of a proposed new capability within the operational framework in which it will perform. It is derived from a higher-level CONOPS and provides a greater level of detail for a specific capability defined in that higher-level CONOPS (*e.g.*, Midterm CONOPS or Service-level CONOPS). The Solution CONOPS communicates top-level quantitative and qualitative characteristics of the solution, and is the foundation for functional analysis and the development of preliminary program requirements. The Solution CONOPS is not based on a particular solution to a service need or shortfall and should be sufficiently flexible to permit the evaluation of a range of alternatives.

Systems Engineering Role

The systems engineer is the technical lead for development of the Solution CONOPS. The systems engineer is also responsible for validating the Solution CONOPS to ensure it fulfills the service capability specified in the Service-level CONOPS.

Activity Inputs

"As-is" and "to-be" Service-level and Enterprise Architectures (EA) (for determining interfaces, operational constraints)
Service-gap analysis products

Activity Output

Solution CONOPS

Potential SEM Chapter Reference

Operational Concept
Validation

Quantify Shortfall

A detailed shortfall analysis quantifies the preliminary shortfall defined during service-gap analysis. The output is a clear understanding of the

magnitude of the problem, its nature, urgency, and impact, as well as a compelling case for why FAA should invest resources to resolve it.

Systems Engineering Role
The systems engineer takes the lead in quantifying the service shortfall as a basis for defining preliminary functional and performance requirements.

Activity Input
Preliminary Shortfall Analysis Report

Activity Output
Detailed Shortfall Analysis Report

Potential SEM Chapter References
Operational Concept
Technical Assessment

Perform Functional Analysis
Functional analysis translates service needs into high-level functions that must be performed to achieve the desired service outcome in every operating environment in which the solution will perform. Functional analysis then decomposes high-level functions into sequentially lower-level sub-functions. Through this process of analyzing and defining functions, a description of the solution emerges that becomes the framework for developing requirements and a physical architecture. It is important that the definition of functions focuses on *what* the new capability will do and *not how* the service will be provided. Potential constraints include environmental, safety, regulatory, interface, security, and performance requirements.

Systems Engineering Role
The systems engineer leads this activity, which includes development of an N^2 diagram and a functional flow block diagram. (See Chapter 12 – Functional and Performance Allocation for examples.) The N^2 diagram is a visual matrix representing interfaces between solution elements. The functional flow block diagram organizes and depicts functions by their logical order of execution. Both diagrams provide a standardized approach for modeling the functional behavior of a solution.

Activity Inputs
“As-is” and “to-be” Service-level and Enterprise Architectures (EA) (for determining interfaces, operational constraints)
Service-gap analysis products

High-level stakeholder requirements (*e.g.*, NAS Requirements Document)

Activity Outputs
N² Diagram
Functional Flow Block Diagram

Potential SEM Chapter Reference
Functional and Performance Allocation

Develop Enterprise Architecture Products
Solution-level enterprise architecture products are "snapshots" of the solution at particular points in time. They show the "as-is" and the "to-be" states of the Enterprise Architecture. Products required during CRD depict specific relationships and summarize information contained in the Solution CONOPS, the Preliminary Program Requirements Document, and the Range of Alternatives. Requirements for specific products differ for NAS and non-NAS initiatives and are subject to tailoring, based on the scope of the initiative.

Systems Engineering Role
The systems engineer supports the Solution-level architect in developing required Enterprise Architecture views in four key areas: vertical integration, horizontal integration, architectural integration, and gap analysis. Vertical integration ensures the Solution-level architecture accommodates a top-down/bottom-up alignment with elements from the Enterprise-level architecture and supports its "parent" in providing NextGen benefits. Horizontal integration identifies linkages and inter-dependencies across other Solution-level and Service-level architectures. Architectural integration identifies linkages between architecture elements in the same architecture. Gap analysis is a comparison of the "as-is" and "to-be" architectures.

Activity Inputs
Inclusion on an Enterprise Architecture Roadmap (output of service-gap analysis)
Solution CONOPS
Functional Analysis
Shortfall Analysis
"As-is" and "to-be" Service-level and Enterprise Architectures (EA) (for determining interfaces, operational constraints)

Activity Outputs

Specific products (also known as views) are specified for each phase of the Acquisition Management System. Products may be removed or added depending on particular needs or constraints.

Potential SEM Chapter References
Interface Management
Information Management
Functional and Performance Allocation

Assess Safety Risk
A safety risk assessment is conducted to determine if the investment initiative affects the NAS, and if so, whether safety risks are introduced as a result of the initiative. One of three safety products is developed depending on impacts to the NAS and resulting safety risks. An Operational Safety Assessment is used when the initiative impacts the NAS and introduces safety risks to the NAS. A Safety Risk Management Decision Memo is used when the initiative impacts the NAS but does not introduce safety risks. A memo to file is used when the initiative does not impact the NAS and does not introduce new safety risks to the NAS. Planning for mitigation of safety risks may result in the addition of safety requirements to the preliminary program requirements document.

Systems Engineering Role
The systems engineer supports the safety team with background information on proposed capabilities and preliminary alternatives so it can assess safety risk accurately. This includes a determination of safety impact and criticality of proposed functions and requirements.

Activity Inputs
Operational environment as described in the Service-level CONOPS and “to-be” Enterprise Architecture
Alternative descriptions of proposed alternatives

Activity Output
Appropriate safety artifact (one of three)

- Operational Safety Assessment
- Safety Risk Management Decision Memo
- Memo to file

SEM Chapter Reference
System Safety Engineering
Information Security Engineering
Hazardous Materials and Environment

Develop Preliminary Requirements

Preliminary program requirements define high-level functional, performance, interface, safety, security, and constraint (*e.g.*, environmental, operational, regulatory) requirements the intended investment must satisfy, while avoiding requirements that are biased toward a specific solution. To the contrary, preliminary requirements should be written to allow unbiased evaluation of various alternative solutions. Excessively detailed preliminary requirements are neither necessary nor desirable.

Systems Engineering Role

Developing preliminary requirements is a collaborative effort that involves users and stakeholders combined with multiple technical and programmatic disciplines. The systems engineer participates in iterative dialogues and communications with stakeholders and discipline subject-matter experts to transpose service needs from the detailed Shortfall Analysis Report into preliminary performance requirements within context of the solution operational architecture that has emerged from the Solution CONOPS and functional analysis.

Activity Inputs

Detailed Shortfall Analysis Report with quantified service needs
Operational environment from Solution CONOPS and functional analysis
N2 diagrams and functional flow block diagrams
Enterprise Architecture views
High-level stakeholder requirements (*i.e.*, NAS Requirements Document)

Activity Output

Preliminary Program Requirements Document

Potential SEM Chapter Reference

Operational Concepts
Requirements Management
Functional and Performance Allocation

Develop Range of Alternatives

Developing a range of distinct alternatives increases the likelihood the best possible solution will be selected to satisfy the service need. Alternatives are technically diverse, qualitatively different, creative, flexible, and innovative. They eliminate or significantly decrease the shortfall. Nonmaterial solutions should be considered (*e.g.*, procedural, personnel, or policy changes). If the "To Be" Architecture contains an alternative, it is evaluated. The legacy case (status quo) is not an alternative, but portrays the current operational

framework against which alternatives are evaluated. However, if modification of a legacy asset mitigates the shortfall, it is evaluated. Acquisition alternatives such as lease-versus-buy are not distinct alternatives. At minimum, three alternatives are required and a preliminary alternative description is developed for each.

Systems Engineering Role
Alternative concepts will have different strengths and weaknesses that present "trade spaces," where decisions can be made among such factors as performance, risk, cost, and benefits. Other key factors to consider are safety, operational cost efficiencies, technological maturity, and impact on the workforce and Enterprise Architecture. The systems engineer plays a key role in evaluating trade-offs among alternatives and the relative strengths and weaknesses of each.

Activity Inputs
Trade studies of various technologies
Vendor ideas
Shortfall analysis describing the service and capability gaps
Desired solution functions
Preliminary program requirements
Potential solution identified in the Enterprise Architecture

Activity Output
Technical descriptions of the three most promising alternatives

Potential SEM Chapter Reference
Decision Analysis

Estimate Costs and Benefits
Rough Life Cycle costs and benefits are developed for each alternative using suitable estimating techniques as a basis for determining whether the alternative should be investigated further or eliminated from consideration. Preliminary alternative descriptions provide the technical basis for estimating both life cycle costs and benefits. Rough Life Cycle costs are also calculated for sustaining the legacy case for its remaining useful life or for the duration of the analysis period of the replacement capability, whichever is shorter.

Systems Engineering Role
The systems engineer ensures all requirements for supporting the solution throughout its life cycle are considered and accounted for in the cost estimate. These life cycle requirements include such items as deployment and transition, integrated logistics support, technology sustainment and evolution, as well as disposal of any asset that is

replaced. The systems engineer also ensures the set of preliminary requirements can be tied to a collection of tangible benefits.

Activity Inputs
Preliminary Alternative Descriptions for the three most promising alternatives
Cost estimates for the existing (legacy) asset, including ongoing operating and maintenance costs

Activity Output
Rough Life Cycle cost and benefit estimates for each alternative

Potential SEM Chapter Reference
Integrated Technical Planning

Compose Investment Analysis Plan
An Investment Analysis Plan is developed to ensure resources are in place to complete the requirements of the investment analysis phase. The plan (1) defines the scope and assumptions of the analysis; (2) describes the alternatives with their associated costs and benefits; (3) defines organizational roles and responsibilities; (4) specifies a target schedule and required work products; and (5) estimates resources needed for the work. By signing the Investment Analysis Plan, the organizations that will conduct the analysis agree to provide the resources necessary to complete the work.

Systems Engineering Role
The systems engineer ensures sufficient engineering resources are included in the plan to complete the activities of investment analysis.

Activity Input
Resource needs and constraints from organizations that will perform investment analysis

Activity Output
Investment Analysis Plan

Finalize Acquisition Category (ACAT) Designation Request
The acquisition category determination request is updated using the life cycle cost and benefits estimates developed for each alternative during concept and requirements definition. The Investment Decision Authority, the board or group of individuals responsible for each investment decision, is based on the final acquisition category designation. The acquisition category assigned to the initiative at this point will carry through the rest of the Acquisition Management System Life Cycle.

Systems Engineering Role
None

Other Systems Engineer Responsibilities During CRD

The systems engineer evaluates preliminary alternatives and requirements for specialty systems engineering disciplines such as reliability, availability, maintenance, human-product interaction, electromagnetic compatibility and interference, information security, and environmental impact (including hazardous material) as a basis for eliminating alternatives that have unacceptable negative attributes and for defining preliminary functional and performance requirements. The systems engineer assists in validating that the Solution CONOPS is aligned with the NexGen Midterm CONOPS and that preliminary program requirements will satisfy crucial stakeholder needs. The systems engineer also identifies and mitigates technical risks that emerge during concept and requirements definition.

Interdependencies

Requirements Management
Interface Management
Risk Management
Configuration Management
Information Management
Technical Assessment
Decision Analysis
Operational Concepts
Functional & Performance Allocations
Human Factors
Information Security
System Safety
Hazardous Materials/Environmental Engineering

References and Tools

Reference or Tool	Description
Service Analysis and Concept and Requirements Definition Guidelines	Instruction, responsible agent, product, approval authority, templates, and supporting tools and guidance for each CRD activity. Templates for ACAT determination request, CRD plan, shortfall analysis report, alternative description, investment analysis readiness decision executive summary and briefing, solution CONOPS, Non-NAS CRD readiness briefing signature.
FAA Acquisition Management System Toolset (FAST) http://fast.faa.gov	CRD policy CRD readiness decision policy IARD policy
NAS Enterprise Architecture Framework (NASEAF) https://nasea.faa.gov/file/get/814	Paragraph 4.1.1 defines the architectural products required during CRD
NAS Requirements Document NAS-RD-2010	These enterprise level requirements establish the top level of a much more detailed requirements database development effort in support of NextGen development and technical management.

21 – Initial Investment Analysis

Introduction

Investment analysis is the third phase within the AMS life cycle. It follows the Concept and Requirements Definition Phase. Investment analysis begins with the investment analysis readiness decision, which determines whether the detailed shortfall analysis, solution CONOPS, preliminary requirements, and initial alternatives are sufficiently defined to warrant entry into investment analysis. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery.

Investment analysis consists of two stages:

- **Initial investment analysis** - Generates the information needed to select the alternative offering the most promising solution to the service shortfall; and
- **Final investment analysis** - Develops preliminary planning and an acquisition program baseline for the alternative selected at the initial investment decision.

Initial Investment Analysis

Figure 21-1 below illustrates the relationships among the entrance criteria, inputs, phase activities, outputs, and systems engineering and specialty processes during initial investment analysis. In the section that follows, each phase activity required by FAA AMS policy is described, along with the specific responsibility of the systems engineer. Useful references and tools follow in the table at the end.

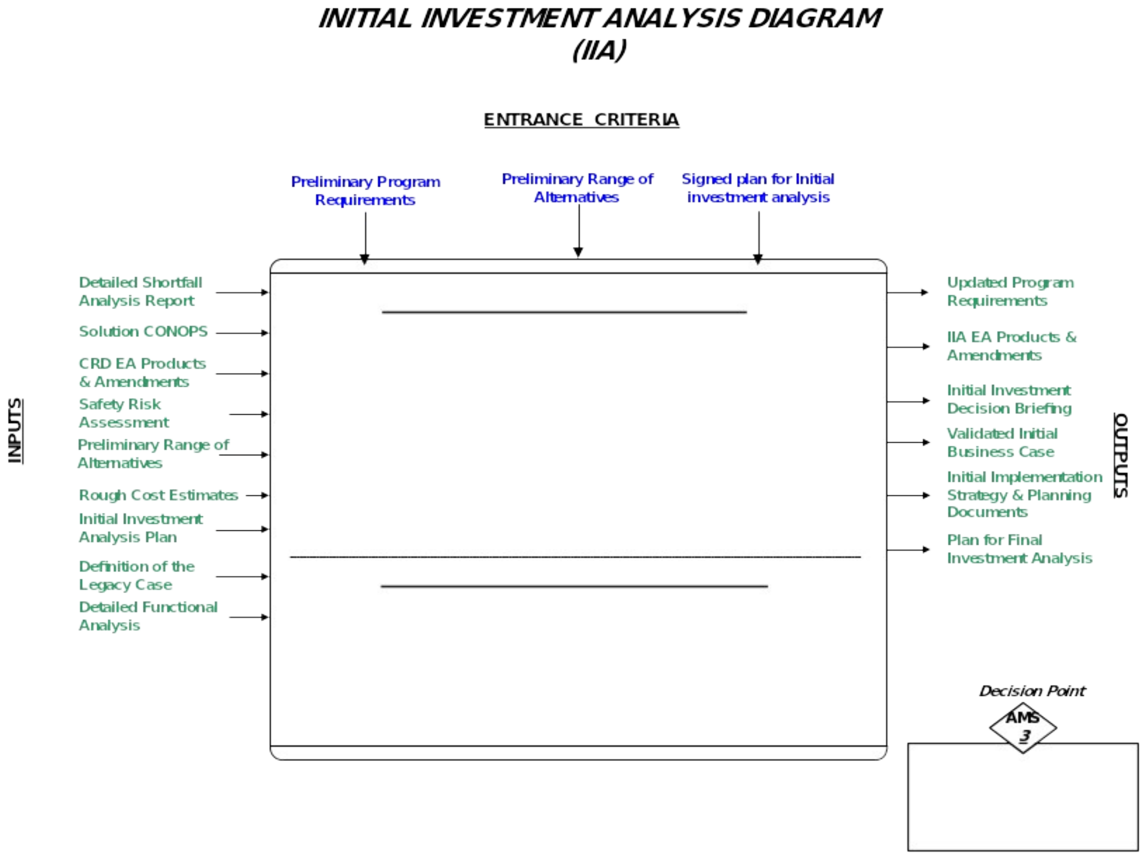


Figure 21-1. Initial Investment Analysis Inputs and Outputs

Initial Investment Analysis Activities

The activities in this process include the following:

- Form Investment Analysis Team
- Define Business Case
- Determine Market Capability
- Analyze Business Case
- Update Program Requirements
- Prepare Initial ISPD
- Develop Final IA Plan
- Validate and Verify Key Work Products

These activities are described below.

Form Investment Analysis Team

The investment analysis plan, developed during concept and requirements definition, specifies members of the investment analysis team. The first order of business after the investment analysis readiness decision is to review the plan and make needed adjustments based on that review. Most important is the schedule and team membership. The team lead requests from management any additional members needed to perform the tasks and complete the products of initial investment analysis within the specified timeframe.

Systems Engineering Role

The systems engineer must ensure sufficient engineering resources are available to the team, to complete the activities and to create the products of initial investment analysis. This may involve establishing commitments from a range of engineering disciplines and organizations for assistance.

Activity Inputs

Initial Investment Analysis Plan

Activity Outputs

Amended Initial Investment Analysis Plan
Amended Team Membership
Commitments for Engineering Support

Potential SEM Chapter Reference

None

Define Business Case

This activity establishes the foundation for determining what information must be gathered and analyzed during initial investment analysis. This may include: refining the performance gap or economic opportunity; determining whether the right problem is being addressed; validating the problem statement with the stakeholders; documenting assumptions, constraints, and policies that govern conduct of the analysis; refining the operational and technical description of the legacy case; or defining which and how agency strategic and performance measures will be impacted by the investment.

Systems Engineering Role

The systems engineer must identify what other programs are impacted by the initiative and describe the impact succinctly. He must then identify other initiatives in the enterprise architecture that also address the shortfall in whole or in part. In addition, he must investigate opportunities for efficiencies to explore during initial investment

analysis. Finally, the systems engineer must assess the potential impact if the initiative is not implemented, is delayed by at least five years, or is partially implemented now and completed at a later date.

Activity Inputs
Shortfall Analysis
Solution CONOPS
Legacy Case
Preliminary Requirements
Preliminary Range of Alternatives
Enterprise Architecture

Activity Outputs
Assumptions, Constraints, Policies
Business Case Analysis Strategy
Investment Decision Criteria

Potential SEM Chapter Reference
Validation
Risk Management

Determine Market Capability
The standard means for gathering market data is a screening information request that defines preliminary requirements and solicits information on potential solutions. The scope of the market search varies, but must always seek the widest possible input from industry and other sources with potential solutions such as government agencies, foreign institutions, or universities.

Systems Engineering Role
The systems engineer must update preliminary program requirements as necessary to provide a complete statement of functional and performance need sufficiently detailed to provide useful direction to respondents of the market survey.

Activity Inputs
Preliminary Requirements
Preliminary Range of Alternatives
Estimated Program Schedule

Activity Outputs
Screening Information Request
Vendor Responses

Potential SEM Chapter References

Information Management
Decision Analysis

Business Case Analysis
Business case analysis (BCA) provides the basis for identifying and selecting the best solution to the service need or shortfall. It documents and links together, in one cohesive story, all key factors that demonstrate the value and worth of a proposed investment to FAA and its customers. Key factors include impact on and contribution to FAA organizational goals and mission responsibilities (Destination 2025); alignment with the Enterprise Architecture and its roadmaps; and life cycle costs and benefits, particularly the potential for lowering operational costs and risk. BCA is tailored according to acquisition category—the more complex and higher value the investment opportunity, the more complex the analysis.

BCA has the following elements: cost, benefit, risk, and schedule. It is supported by the following engineering assessments: requirements sensitivity, technological maturity, specialty engineering, architecture impact, human engineering and operability, information and security, and environment and occupational safety and health. Consult the investment analysis and business case guidelines and other specialty guidance listed in the references and tools table at the end of this chapter for detailed information concerning the conduct of initial investment analysis.

Systems Engineering Role
The systems engineering role during business case analysis is substantial and complex. It consists of the following four assessments:

- *Requirements Assessment:* Identify key requirements that drive costs and benefits. Analyze sensitivity of requirements on cost and capability. Rank alternatives against critical performance requirements and positive impact on targeted FAA performance measures. Determine if business process re-engineering can reduce/relax requirements or lower costs.
- *Technological Maturity Assessment:* Review the technological maturity of each alternative and assess associated risks on cost, performance, and schedule.
- *Architecture Impact Assessment:* Describe how the investment opportunity supports the FAA Enterprise Architecture and whether it supports the Federal Enterprise Architecture. Categorize the proposed investment as necessary to solve a critical problem, increase efficiency or provide better service.
- *Specialty Engineering Assessment:* Ensure the following specialty engineering topics are integrated into the overall assessment of alternatives: Reliability, maintainability, availability; radio

frequency management; environmental impact; supportability and integrated logistics support; NAS quality assurance and performance; enterprise configuration management and operations. The specialty engineering assessment includes the following three sub-assessments:

- Human Engineering/Operability Assessment: Analyze the full range of human factors and interfaces (*e.g.*, cognitive, organizational, physical, functional, environmental) necessary to achieve an acceptable level of performance for operating, maintaining, and supporting the solution over its service life.
- Information Security Assessment: Ensure information technology security requirements and life cycle costs are identified, assessed, and validated.
- Environment and Occupational Safety and Health Assessment: Ensure safety-related items on the investment decision authority (IDA) readiness checklist have been completed.

Activity Inputs
Shortfall Analysis
Solution CONOPS
Legacy Case
Preliminary Requirements
Preliminary Range of Alternatives
ROM Costs
Monetized Value of Shortfall
Initial Screening Information Request Results
Estimated Program Schedule
Assumptions, Constraints, and Policies
Safety Risk Assessment

Activity Output
Initial Business Case
Engineering Assessments
Recommended Alternative
Updated Enterprise Architecture Products
Risk-Adjusted Life Cycle Costs
Cost Basis of Estimate
Risk-Adjusted Life Cycle Benefits
Benefits Analysis Report
Risk Assessment

Potential SEM Chapter Reference
Technical Assessment
Decision Analysis
Verification
Human Factors
Information Security Engineering
Electromagnetic Environmental Effects and Spectrum Management

Update Program Requirements
Vendor responses are assessed against preliminary requirements to determine whether relaxation or modification would enable promising concepts to be acceptable for implementation. The objective is to identify solutions that may not fulfill all requirements, but are diverse, innovative, and have a positive impact on targeted FAA performance without compromising essential stakeholder needs.

Systems Engineering Role
The systems engineer must use input from key stakeholders and vendor proposals to refine requirements to lower cost or risk, or increase performance and benefits while retaining critical performance needs.

Activity Inputs
Preliminary Program Requirements
Vendor Information
Engineering and Stakeholder Assessments
Initial Business Case

Activity Output
Updated Program Requirements

Potential SEM Chapter Reference
Functional & Performance Allocation
Requirements Management
Verification

Prepare Initial Implementation Strategy and Planning Document (ISPD)
An abridged implementation strategy and planning document is developed for each alternative during initial investment analysis to highlight any special features or circumstances that would impact cost and schedule; for example, data rights, supportability issues, obsolescence, configuration management, and costs associated with use of Non-Developmental Items (NDI) or Commercial, Off-the-Shelf (COTS) components. The ISPD template on the

FAA Acquisition System Toolset website (http://fast.faa.gov) defines exactly which sections are completed. These initial plans constitute a basis for determining which alternative the investment decision authority should select.

Systems Engineering Role
The systems engineer must define the scope and complexity of systems engineering associated with each alternative. Estimate how differences will impact such factors as cost, schedule, risk, reliability, maintainability, availability, configuration management, human integration, manpower, documentation, interfaces, and specialty engineering.

Activity Inputs
Engineering Assessments
Results of Initial Screening Information Request
Results of Trade Studies

Activity Output
Initial Implementation Strategy and Planning Document for Each Alternative

Potential SEM Chapter Reference
Solution Implementation

Develop Plan for Final Investment Analysis
The final investment analysis (FIA) plan defines entrance criteria for the final investment decision; participating organizations and team members; all work activities, resources, schedules, roles and responsibilities; and products. It includes necessary risk-reduction activity such as modeling, analysis, simulation, or research. The FIA plan also includes procurement activity associated with the release of a screening information request seeking proposals for solution implementation and the resultant evaluation effort. The plan also specifies when the results of the analysis are to be completed for a final investment decision.

Systems Engineering Role
The systems engineer assists the team in preparing the plan for final investment analysis, making sure sufficient engineering resources are included to complete such tasks as developing the product specification and screening information request for vendor proposals. He must also ensure completion of the development of an implementation-strategy-and-planning document and work breakdown structure for the selected alternative.

Activity Inputs
Stakeholder Organization Resource Requirements for Final Investment Analysis

Activity Output
Plan for Final Investment Analysis

Potential SEM Chapter Reference
None

Validate and Verify Key Documents
Program requirements and the initial business case are verified and validated to ensure a sound basis for selection of the best alternative for implementation. This evaluation ensures business case estimates were developed using sound practices and are logical and realistic. It provides the investment decision authority with a "cross check" of the work performed and reduces risk associated with the investment decision. Business case validation is conducted as described in "AJF Business Case Evaluation and Assessment Guideline."

Systems Engineering Role
Evaluate whether the degree to which each alternative will satisfy program requirements (*e.g.*, performance, availability, compatibility, transportability, interoperability, reliability, maintainability, safety, human factors, logistics supportability, documentation, staffing, personnel, and training) is clearly expressed and supported by rigorous analysis. Verify and validate that these factors are correctly specified in the updated program requirements document.

Activity Input
Initial Business Case
Updated Program Requirements
Risk-Adjusted Life Cycle Costs
Cost Basis of Estimate
Risk-Adjusted Life Cycle Benefits
Benefits Analysis Report
Risk Assessment

Activity Output
Verified Initial Business Case
Verified Program Requirements
Validated Problem Statement

Potential SEM Chapter Reference
Validation
Verification

Prepare for Initial Investment Decision
When the business case is sufficiently mature, results and recommendations are presented to the investment decision authority for approval. The following are completed before this decision: decision materials; IDA readiness checklist; verification that initial investment decision exit criteria are satisfied; coordination of findings and recommendations with stakeholders; identification of issues or concerns; briefing to the IDA financial review authority; concurrence to present the business case to the investment decision authority; and approval of subordinate review board, and pre-brief of IDA members, as requested.

Systems Engineering Role
The systems engineer must provide the basis for evaluating and selecting alternatives. Decision criteria are specified in AMS policy section 2.4.4.

Activity Input
Validated Initial Business Case
Updated Program Requirements
Preliminary ISPD for Each Alternative

Activity Output
Initial Investment Decision Briefing Package

Potential SEM Chapter Reference
Technical Assessment
Decision Analysis

Interdependencies

Integrated Technical Planning
Requirements Management
Interface Management
Risk Management
Configuration Management
Information Management
Technical Assessment
Decision Analysis
Operational Concepts
Functional & Performance Allocations
Human Factors
Information Security
System Safety
Hazardous Materials/Environmental Engineering

References and Tools

Reference or Tool	Description
System Engineering Manual	Requirements Management Functional Analysis Trade Studies Specialty Engineering Risk Management Validation and Verification
FAA Acquisition Management System Toolset (FAST) http://fast.faa.gov	Investment Analysis Standard Guidance Investment Analysis Process Guidance Business Case Analysis Guidance and Template
NAS Enterprise Architecture Framework (NASEAF) Apr 23, 2007	
Investment Planning & Analysis Web Site http://www.ipa.faa.gov	Investment Analysis Processes and Products Building the Business Case Methodologies: Cost Analysis, Benefits Analysis, Economic Analysis, Risk Analysis, Schedule Analysis Communicating Your Business Case Evaluating the Business Case Business Case Guidelines & Templates Guidelines for Conducting Shortfall Analysis Guidelines for Defining and Applying the Legacy Case Investment Analysis Plan Guidelines and Template Guidelines for Defining and Determining the Required Service Period, Economic Service Life, and Analysis Period Guidelines for FAA Cost Estimating Guidelines for Documenting Cost Basis of Estimate Guidelines for Benefits Estimating and Report Template Guidelines for Conducting Investment Analysis Risk Assessment AJF Business Case Evaluation and Assessment Guideline

22 – Final Investment Analysis

Introduction

Investment analysis is the third phase within the AMS life cycle. It follows the Concept and Requirements Definition Phase. Investment analysis begins with the investment analysis readiness decision, which determines whether the detailed shortfall analysis, solution CONOPS, preliminary requirements, and initial alternatives are sufficiently defined to warrant entry into investment analysis. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery.

Investment analysis consists of two stages:

- **Initial investment analysis** - Generates the information needed to select the alternative offering the most promising solution to the service shortfall; and
- **Final investment analysis** - Develops preliminary planning and an acquisition program baseline for the alternative selected at the initial investment decision.

Final Investment Analysis

The objective of final investment analysis is to mature the alternative selected at the initial investment decision into a low-risk, successful FAA investment program ready for solution implementation. This is accomplished through a set of integrated activities that focus on three goals:

- Reduce investment risk
- Begin procurement of the new asset
- Plan for solution implementation

Figure 22-1, below, illustrates relationships among the entrance criteria, inputs, phase activities, outputs, and systems engineering functions during final investment analysis. In the sections that follow, each activity phase required by AMS policy is described along with the specific responsibility of the systems engineer. References and tools follow in the table at the end.

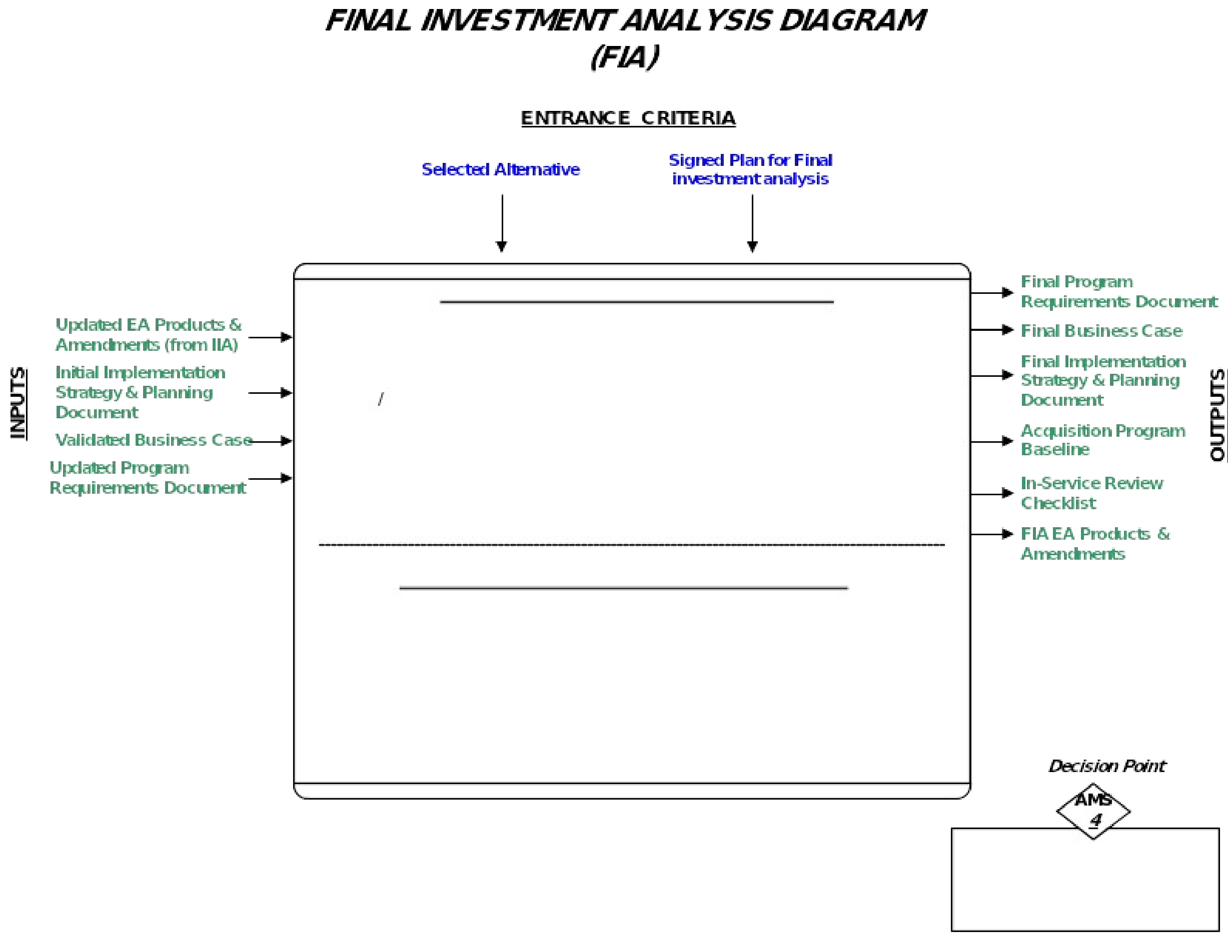


Figure 22-1. Final Investment Analysis Inputs and Outputs

Final Investment Analysis Activities

The activities in this process include the following:

- Identify Key Planning Elements
- Reduce Risk and Finalize Requirements
- Finalize Strategy for Implementation and Life Cycle Support
- Solicit/Evaluate Offers for Prime Contract
- Develop Detailed Program Planning
- Finalize Business Case
- Establish Acquisition Program Baseline
- Verify and Validate Key Work Products

These activities are described below.

Identify Key Planning Elements
All actions and events necessary to obtain and support the solution over its life cycle are identified as a basis for detailed program planning during final investment analysis. Extensive liaison across FAA is required to determine the full range of tasks and activities (*e.g.*, logistics support, configuration management, test and evaluation, information security, system safety, human factors, physical infrastructure, and telecommunications) necessary to achieve efficient delivery and life cycle support for the solution selected for implementation. The final investment analysis plan is evaluated and revised, if required, to ensure it supports the full range of activity necessary to reduce risk and plan the investment initiative thoroughly.

Systems Engineering Role
The systems engineer ensures sufficient engineering resources are available to complete the activities of final investment analysis. This may involve establishing commitments from multiple engineering disciplines and organizations.

The systems engineer also ensures the key engineering activities and actions that must be completed during solution implementation to obtain, deploy, and support the solution over its intended service life are included in program planning and budgeting documents.

Activity Inputs
Signed Plan for Final Investment Analysis
Selected Alternative

Activity Outputs
Revised Plan for Final Investment Analysis
Preliminary Program Work Breakdown Structure

Potential SEM Chapter Reference
Integrated Technical Planning

Reduce Risk and Finalize Requirements
Risks associated with the proposed solution that threaten performance, cost, schedule, and benefit objectives are examined in greater depth during final investment analysis. For example, concept feasibility may be evaluated through prototype demonstration or realistic modeling; commercial, off-the-shelf components may be evaluated by means of an operational capability demonstration. For known risks that will be carried into solution implementation, risk-mitigation strategies are documented in the Program

Management section of the Implementation Strategy and Planning document; risk mitigation costs and schedules are embedded in the Acquisition Program Baseline.

After completion of risk-management planning and risk-reduction activity, final quantified operational and performance requirements are recorded in the final program requirements document. Solution performance is evaluated against these measures during operational testing to determine operational suitability and effectiveness.

Systems Engineering Role

The systems engineer leads activity to identify and assess technical risks associated with the solution and to define appropriate risk mitigation strategies. These strategies are a starting point for risk-mitigation planning that supports management decisions on performance, schedule, and cost. The outputs of this process are shared with stakeholders to achieve alignment and acceptance of resource and schedule recommendations, as well as agreement on residual risk that will be carried into solution implementation for resolution.

The systems engineer leads review of the solution functional baseline to ensure there is mutual agreement between the implementing service organization and operational stakeholders concerning the capability that will be obtained during solution implementation.

Finally, the systems engineer leads review of final program requirements to ensure they are completely and properly defined. This review establishes the final requirements baseline as recorded in the final program requirements document.

Activity Inputs

Updated Program Requirements

Activity Outputs

Final Program Requirements Document
Final Functional/Performance Specification

Potential SEM Chapter Reference

Requirements Management
Risk Management

Finalize Strategy for Implementation and Life Cycle Support
The FAA standard work breakdown structure is used as a basis for developing the overall strategy for procuring, implementing, and supporting the solution over its life cycle. Results are recorded in the implementation strategy and planning document, which includes the roles and responsibilities of individuals and organizations critical to program success.

System Engineering Role
The system engineer defines discrete life cycle management activities for engineering disciplines consistent with the FAA standard work breakdown structure, such as human factors, configuration management, reliability, maintainability, and availability. These elements are integrated into all other program planning activities as a basis for developing cost and schedule estimates and detailed planning for the solution.

Activity Inputs
Selected Alternative
Initial Implementation Strategy and Planning Document

Activity Outputs
Final Implementation Strategy

Potential SEM Chapter References
Integrated Technical Planning

Solicit/Evaluate Offers for Prime Contract
A screening information request for the needed capability is released and industry responses are evaluated during final investment analysis. These steps are to ensure the costs and schedules contained in the Implementation Strategy and Planning document and Acquisition Program baseline are of sufficient accuracy to enable the solution to be obtained, deployed, and maintained over its projected service life (within approved cost, schedule, and performance values). *Note that a request for offer may be released only after the initial investment decision and a contract award must not be made until after the final investment decision.*

A statement of work, final functional/performance specification, and contract terms and conditions are prepared for the selected alternative and are included in the screening information request. A contract-specific independent government cost estimate is prepared to assist in evaluating contract proposals.

A source selection team evaluates technical proposals received from bidders and compares them to the screening information request. The source selection team then compares bidder proposals to government estimates of cost, benefits, schedules, and risks. If appropriate, the team adjusts its risk-management planning and proposed baselines to reflect its assessment as to whether bidder estimates are more realistic than its own estimates.

Systems Engineering Role

The systems engineer assists the service organization with preparation of the statement of work, final functional/performance specification, and contract terms and conditions. The systems engineer uses input from key stakeholders and vendor proposals to refine requirements to lower cost or risk or increase performance and benefits while retaining critical performance needs. The systems engineer assists with development of the independent government cost estimate and with technical evaluation of vendor proposals.

Activity Inputs

Final Functional/Performance Specification
Final Program Requirements Document
Final Implementation Strategy

Activity Output

Independent Government Cost Estimate
Screening Information Request
Vendor Proposals
Evaluated Vendor Proposals

Potential SEM Chapter Reference

None

Develop Detailed Program Planning

The actions and activities necessary to implement the investment initiative are recorded in the Implementation Strategy and Planning document. This planning is developed using the standard FAA work breakdown structure (WBS) and a tailored, In-Service Review checklist. All activities and tasks essential to solution development, deployment, and life cycle operation and support are planned. Within the WBS, tasks are described in sufficient detail that resources and schedules can be determined and recorded in the final business case and acquisition program baseline. Schedules for each WBS element and an integrated network schedule for the entire investment program are developed. The structure and mechanisms by which the investment program will be controlled are established using the principles of FAA earned value management policy.

Systems Engineering Role
The systems engineer identifies and specifies actions and activities necessary to accomplish all engineering aspects of solution implementation. The systems engineer also ensures sufficient engineering resources and schedules are included in program planning and budget documents. The systems engineer assists the service organization with developing a program management measurement structure for application during solution implementation that embodies the principles of FAA's earned value management policy.

Activity Inputs
Strategy for Implementation and Life Cycle Support

Activity Output
Final Implementation Strategy and Planning Document
Program Management Measurement Structure

Potential SEM Chapter Reference
Integrated Technical Planning

Finalize the Business Case
The final business case demonstrates the value of implementing the proposed investment program and specifies the resources, budgets, schedules, and contract baseline(s) required to implement the solution. It is presented to the investment decision authority at the final investment decision. The final business case requires computation of the following economic measures: risk-adjusted cost, net present value, cost-benefit ratio, and payback period.

Systems Engineering Role
The systems engineer thoroughly analyses the alternative selected for implementation to ensure performance specifications are consistent with final program requirements and that implementation strategy and planning conform to agency standards and specifications. The systems engineer participates in sensitivity analyses to examine how variations in reliability, maintainability, availability, configuration management, human integration, manpower, documentation, interfaces, and specialty engineering affect solution cost, schedule, and risk. The systems engineer finalizes enterprise architecture artifacts required for a final investment decision.

Activity Inputs
Initial Business Case

Updated EA Products & Amendments
Selected Alternative
Selected Vendor Proposal
Revalidated Shortfall
Final Implementation Strategy and Planning Document
Final Program Requirements Document
Final Functional/Performance Specification

Activity Output
Final Business Case
Activity Spend Plan
Final EA Products & Amendments

Potential SEM Chapter Reference
Configuration Management

Establish Acquisition Program Baseline
The acquisition program baseline establishes cost, schedule, and performance targets to which the implementing service organization is held accountable and against which the program will be measured. See*:* *FAA Acquisition Baseline Management Standard Operating Procedure*, *March 18, 2009*.

Systems Engineering Role
After vendors respond to the screening information request, the systems engineer uses those responses and the final business case to assist the implementing service organization develop cost, schedule, and performance values for the acquisition program baseline. The goal is to produce a baseline of sufficient accuracy to enable the solution to be obtained and deployed within approved cost, schedule, and performance values.

Activity Inputs
Screening Information Request Responses
Final Business Case

Activity Output
Acquisition Program Baseline

Potential SEM Chapter Reference
None

Verify and Validate Key Work Products

The primary focus of verification and validation during final investment analysis is to validate the final business case, final requirements document, program planning, and acquisition program baseline to ensure a solid foundation for implementation of the solution. This evaluation ensures business case estimates were developed using sound practices and are logical and realistic. It provides the investment decision authority with an independent assessment of the work performed during final investment analysis and reduces risk associated with the investment decision. Business case validation is conducted as described in *AJF Business Case Evaluation and Assessment Guideline.* Verification and validation for all other program documentation is conducted as described in FAA AMS Life Cycle Verification and Validation Guidance Document.

Systems Engineering Role

The systems engineer leads verification and validation of final program requirements and the degree to which the solution will satisfy them (*e.g.*, performance, availability, compatibility, transportability, interoperability, reliability, maintainability, safety, human factors, logistics supportability, documentation, staffing, personnel, and training). The systems engineer verifies that engineering costs and activities are adequately specified in program planning and budgeting documents.

Activity Input

Final Business Case
Final Implementation Strategy and Planning Document
Acquisition Program Baseline
Final Program Requirements Document
EA Products and Amendments

Activity Output

Verified and Validated Final Business Case
Verified and Validated Final Implementation Strategy and Planning Document
Verified and Validated Final Acquisition Program Baseline
Verified and Validated Final Program Requirements Document
Verified and Validated EA Products and Amendments

Potential SEM Chapter Reference

Verification
Validation

Assess Budget Impact

The estimate of the life cycle cost and activity spending plan are forwarded to the appropriate investment decision authority finance office. This office assesses the budget impact and contribution to agency goals of the proposed investment against other ongoing and proposed programs in the FAA financial baseline. When an investment initiative cannot be funded within the financial baseline, the finance office may propose offsets from lower priority programs.

Systems Engineering Role

In a constrained resource environment, the systems engineer may be called upon to evaluate the relative contribution to agency goals of the proposed investment initiative against other ongoing and proposed programs and to identify possible funding offsets from lower priority programs.

Activity Input

Final Business Case
Activity Spend Plan

Activity Output

Budget Impact Assessment

Potential SEM Chapter Reference

None

Finalize In-Service Review Checklist

The In-Service Review (ISR) checklist is a deployment planning tool for identifying, documenting, and resolving deployment and implementation issues. It is developed during final investment analysis and serves as a basis for detailed planning for solution implementation and life cycle support, as well as for determining readiness for an in-service decision.

Systems Engineering Role

The systems engineer participates in the ISR checklist tailoring process to ensure all key aspects of fielding a new capability and sustaining it over its service life are addressed in solution planning and funding documents so deployment will not create a critical deficiency in the National Airspace System.

The system engineer ensures all engineering activities associated with developing, installing, testing, and transition from legacy assets to the new operational capability are included in implementation plans and budgets.

Activity Input
Final Implementation Strategy and Planning Document

Activity Output
In-Service Review Checklist

Potential SEM Chapter Reference
None

Interdependencies

Integrated Technical Planning
Requirements Management
Interface Management
Risk Management
Configuration Management
Information Management
Technical Assessment
Decision Analysis
Operational Concepts
Functional & Performance Allocations
Human Factors
Information Security
System Safety
Hazardous Materials/Environmental Engineering

References and Tools

Reference or Tool	Description
FAA Acquisition Management System (AMS) Toolset (FAST) Acquisition Management Policy Section 2.4 Investment Analysis http://fast.faa.gov	AMS Policy establishes all requirements for acquisition management at FAA. Specifically it describes the activities that must be completed, the outputs and products of each activity, who is responsible, and who approves.
FAA Acquisition Management System Toolset (FAST) http://fast.faa.gov	Investment Analysis Standard Guidance Provides guidance, instructions, and templates for final investment analysis.
NAS Enterprise Architecture Framework (NASEAF) Apr 23, 2007	Specifies and describes the EA products and amendments that must be developed during final investment analysis.
Investment Planning & Analysis Web Site http://www.ipa.faa.gov	Detailed guidance, templates and instructions for Final Investment Analysis and how to prepare a Business Case Analysis Investment Analysis Processes and Products.

23 – Solution Implementation

Introduction

Solution Implementation is the fourth phase of the AMS life cycle and follows the Investment Analysis Phase. The Solution Implementation phase of AMS begins with the final Investment decision, during which an acquisition program is established for the solution selected and ends when the new capability goes into service (*i.e.*, when a new service or capability is commissioned into operational use at all sites).

Figure 23-1, below, illustrates relationships among the entrance criteria, inputs, phase activities, outputs, and systems engineering functions during final investment analysis. In the section that follows, each phase activity required by AMS policy is described along with the specific responsibility of the systems engineer. Useful references and tools follow in the table at the end.

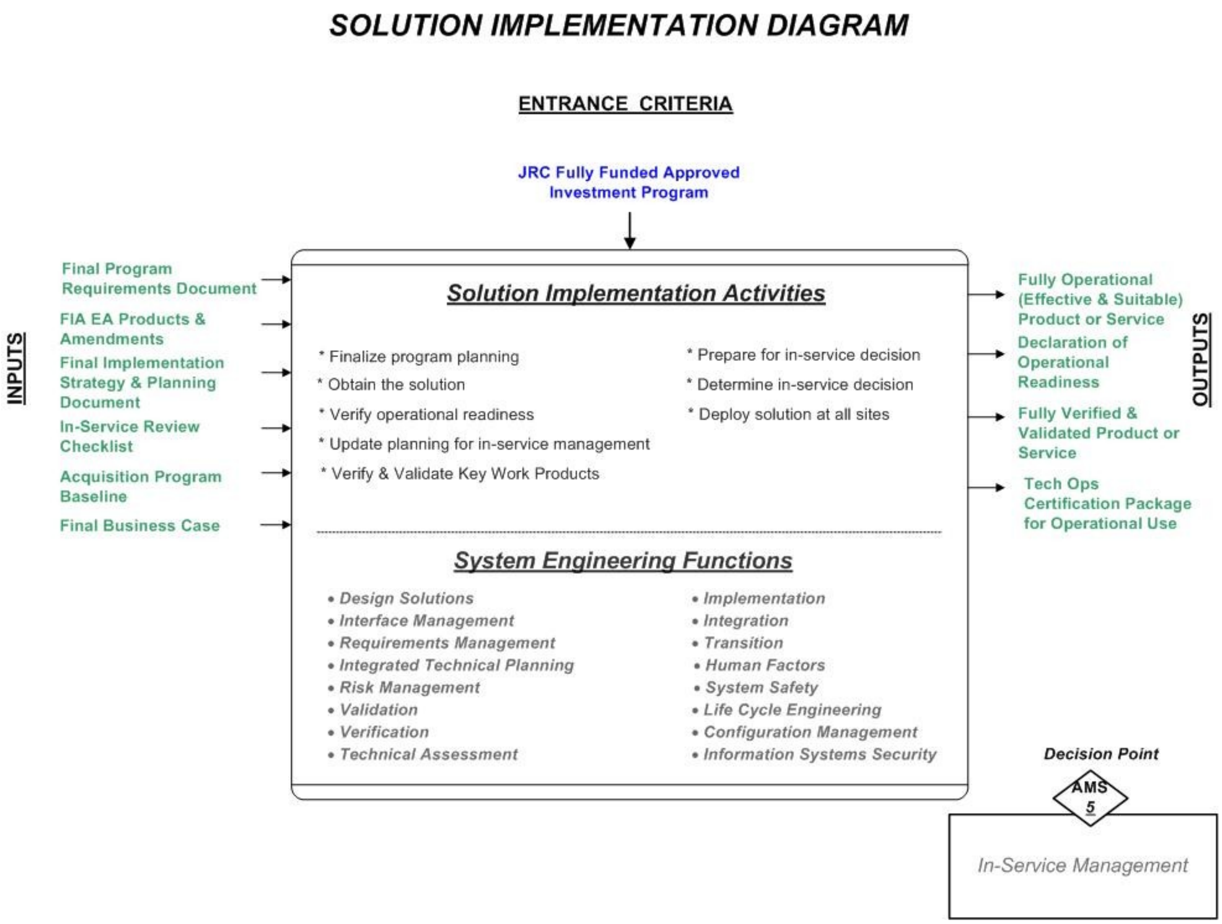


Figure 23-1. Solution Implementation Inputs and Outputs

Solution Implementation Activities

The activities in this process include the following:

- Finalize Program Planning
- Obtain Solution
- Validate Operational Readiness
- Update Planning for In-Service Management
- Verify and Validate Key Work Products
- Prepare for In-Service Decision
- Determine In-Service Decision
- Deploy Solution at All Sites

These activities are described below.

Finalize Program Planning

Key program stakeholders work with the service team to ensure implementation planning is complete and realistic. Typically, this involves translating the overall strategy in the Implementation Strategy and Planning Document, developed during final investment analysis, into discipline-specific planning for all aspects of program implementation and life cycle support. Examples include a Test and Evaluation Master Plan, Systems Engineering Master Plan, Configuration Management Plan, Logistics Support Plan, and so on. The number and complexity of these plans depend on program complexity. It is crucial to clearly define the role of each government organization and contractor that will participate in program execution. For example, if new systems are to be installed or existing facilities modified, service organization planners must work with service-area offices so people and resources will be available when needed.

Systems Engineering Role

The systems engineer ensures technical program planning is sufficient and addresses all systems engineering disciplines necessary for obtaining the solution. The systems engineer has the following duties:

- Develops and maintains the Systems Engineering Management Plan;
- Participates in post-award conferences to ensure a mutual understanding of requirements;
- Establishes an initial set of technical measures to monitor and control the program;
- Baselines technical risks and develops mitigation plans;
- Establishes entry and exit criteria for technical reviews;

- Identifies independent subject-matter experts for participation in technical reviews;
- Assists in developing Integrated Master Schedule tasks and resulting technical products; and
- Prepares for the Integrated Baseline Review.

Activity Inputs
Implementation Strategy and Planning Document

Activity Outputs
Detailed program planning documents

Potential SEM Chapter Reference
Integrated Technical Planning

Obtain Solution
This activity includes all tasks necessary to develop the solution to the point where it is ready to be verified and validated for operational use. Although dependent on the nature, scale, and complexity of the investment program, obtaining the solution typically includes such activities as contract award, contract administration, program management, resource management, risk management, systems engineering, logistics support, test and evaluation, site acquisition and adaptation, and all contractor and government activity needed to get the solution ready for operational use. This may also involve developing operational procedures and standards; obtaining physical, personnel, and information security; modifying the physical infrastructure; and coordinating collateral action by the aviation industry.

Systems Engineering Role
The systems engineer is the technical subject-matter expert for the program. This role entails participating in user interviews, rapid prototyping, demonstrations, or any other activity that gives confidence the requirements are well understood, consistent, and appropriate before starting detailed design. The systems engineer oversees and monitors program design reviews such as the system design review, preliminary design review, and critical design review. The system engineer also reviews and approves technical contract deliverables.

Activity Inputs
Detailed program planning documents
Program Requirements Document

Activity Outputs

System Requirements Specification; System/Subsystem Specification; Subsystem Design(s); subsystem description(s); Requirements Traceability Matrix; Interface Requirements Document; Software Requirements Specification; Hardware Requirements Specification, System Architectural Design Document; simulations and models; measurements; estimates for system size, schedule, and cost; risk analysis report and risk mitigation plan; source code and databases, updated software development plans; and a fully integrated and tested product or service.

Potential SEM Chapter Reference
Risk Management
Technical Assessment
Requirements Management
Interface Management
Design Solution
Human Factors
System Safety
Information Systems Security
Verification
Integration

Validate Operational Readiness
This includes all activity necessary to install the solution at a designated test site(s) and evaluate it thoroughly to validate operational readiness. Operational readiness encompasses operational effectiveness and operational suitability. Operational effectiveness measures how well the solution satisfies service need and operational requirements. Operational suitability measures how well a product is integrated within its intended environment and prepared for field use, considering such factors as compatibility, reliability, human performance factors, maintenance and logistics support, safety, and training. A declaration of operational readiness date (ORD) and commissioning is required before a solution can be placed into operational use.

Systems Engineering Role
The systems engineer ensures activities and resources for the operational readiness evaluation are sufficient to accomplish the goals of the effort. The systems engineer ensures (based on the contractually-required activities) that the prime contractor demonstrates conformance to contract specifications, which results in government acceptance.

Activity Inputs

Operationally suitable and effective solution
Complete operational support package

Activity Outputs
Validated operational solution
Validated operational support package

Potential SEM Chapter References
Validation

Update Planning for In-Service Management
This activity establishes how the solution will be sustained and managed throughout its service life cycle. It focuses on in-service support, but includes post-implementation review and periodic evaluation of operational assets to measure performance and supportability trends in support of service-level reviews, product-sustainment strategy, service-life extension, and eventual removal from service, including site restoration.

Systems Engineering Role
The systems engineer ensures technical planning for sustaining the solution through its planned service life is sufficient and feasible and that it addresses all necessary systems engineering disciplines. The systems engineer reviews and updates life cycle technical planning documents such as preventive and corrective maintenance, supply chain management, second-level maintenance, and hardware and software depot support. The systems engineer also verifies that the planned life cycle support and management structure is being realized (*e.g.*, maintenance resource requirements, spare/repair parts, test and support equipment, personnel quantities and skills, training resource requirements, environment, safety, health, etc.), and evaluates plans for decommissioning replaced operational assets while considering environmental laws, regulations, and directives.

Activity Inputs
In-service Checklist

Activity Output
Complete and sufficient planning package for in-service technical support for the solution

Potential SEM Chapter Reference
Integrated Technical Planning
Life Cycle Engineering

Verify and Validate Key Work Products
(Occurs throughout the "Obtain the Solution" activity)
The key work products and products of solution implementation are verified and validated as meeting requirements and agency service needs throughout solution implementation. Key work products include the contract/statement of work, design documents, and specifications. End-products are the actual products or services that go into operational use. Verification activity supports contract award, preliminary and final design reviews, product demonstration and production decisions, solution acceptance, and the in-service decision.

Systems Engineering Role
The systems engineer assists in verifying and validating key work products during solution implementation. The scope of verification and validation activity will vary, based on program complexity and available resources.

Activity Inputs
Key work products and products as follows:
System Requirements Specification
System/Subsystem Specification
Subsystem description(s)
Requirements Traceability Matrix
Interface Requirements Document
Software Requirements Specification
Hardware Requirements Specification

Activity Output
Verified and validated solution work products and products

Potential SEM Chapter Reference
Verification
Validation

Prepare for In-Service Decision
This activity includes resolution of all support issues identified by the operating service organization and integrated logistics management team; completion of management actions arising from the in-service review checklist and the independent operational analysis report (designated programs only); resolution of stakeholder issues; development of the in-service decision briefing and action plan; and concurrence of key stakeholders.

Systems Engineering Role
The systems engineer supports the program manager technically and programmatically in all aspects of obtaining a favorable decision from the In-Service Decision authority.

Activity Inputs
Key work products and products of the solution

Activity Output
Verified and validated solution and in-service support package for in-service management

Potential SEM Chapter Reference
TBD

Determine In-Service Decision
The in-service decision authority determines whether the solution and its support package are sufficient for deployment into the operational environment and ready for operational use.

Systems Engineering Role
None

Activity Input
A solution in-service support package, verified and validated as ready for operational use

Activity Output
A management decision on whether to authorize a solution for deployment into the operational environment

SEM Chapter Reference
None

Deploy Solution at All Sites
This includes all activity necessary to install the solution at each site and bring it into operational use. This may involve transportation and delivery of equipment to each site, installation and checkout, contractor acceptance and inspection, integration with other assets, field familiarization, declaration of initial operational capability, joint acceptance and inspection, dual operations, declaration of operational readiness, and removal and disposal of obsolete equipment. The transition from solution implementation to in-service management extends over time, occurring at each site upon declaration of operational readiness or commissioning.

Systems Engineering Role
The systems engineer ensures all activities necessary to transport, deliver, receive, process, assemble, install, checkout, train, operate, house, store, or field the solution to achieve full operational capability are completed and operating efficiently.

Activity Input
Solution and support package authorized for operational use

Activity Output
Installed solution and support package verified and validated for operational use at each operational site

SEM Chapter Reference
Transition Process

Interdependencies

Integrated Technical Planning
Requirements Management
Interface Management
Risk Management
Configuration Management
Information Management
Technical Assessment
Decision Analysis
Operational Concepts
Functional & Performance Allocations
Design Solution
Implementation
Integration
Verification
Validation
Deployment and Transition
Special Consideration for System of Systems
Reliability, Maintainability, and Availability
Life Cycle
EEE and Spectrum
Human Factors
Information Security
System Safety
Hazardous Materials/Environmental Engineering

References and Tools

Reference or Tool	Description
FAA Acquisition Management System Toolset (FAST) Acquisition Management Policy Section 2.5 Solution Implementation http://fast.faa.gov	AMS Policy establishes all requirements for acquisition management over the full life cycle at FAA. Specifically, it specifies requirements for the activities that must be completed during solution implementation, the outputs and products of each activity, the responsible agent or agents, and who approves each output.
FAA AMS Life Cycle Verification and Validation Guidelines	This document guides the application of verification and validation policies across FAA. It defines terminology and illustrates how to accomplish verification and validation and in each phase of the AMS Life Cycle.
NextGen and Operations Planning Services, Test and Evaluation Handbook, document number VVSPT-A2-PDD-013	This document provides detailed guidance as to how to conduct Test and Evaluation for NAS-related systems.
Solution Implementation Acquisition Practices Toolkit https://employees.faa.gov/org/linebusiness/ato/operations/technical_operations/best_practices/Life Cycle/solution_implementation/	This toolkit contains processes, flowcharts, activities, checklists, good examples of works products, and other tools helpful to service team members executing solution implementation.

This page intentionally left blank.

24 – In-Service Management

Introduction

In-service management is the fifth and final phase of the AMS Life Cycle. It follows the Solution Implementation Phase and involves two distinct sets of work activities. The first set monitors and assesses real-world performance of operational assets against baseline requirements and expected benefits, and takes action to optimize performance throughout their operational life. The second set of activities operates and maintains operational assets and their physical and support infrastructure throughout their service life.

Figure 24-1, below, illustrates relationships among entrance criteria, inputs, phase activities, outputs, and systems engineering functions during in-service management. In the section that follows, each phase activity required by AMS policy is described, along with the specific responsibility of the systems engineer. References and tools follow in the table at the end.

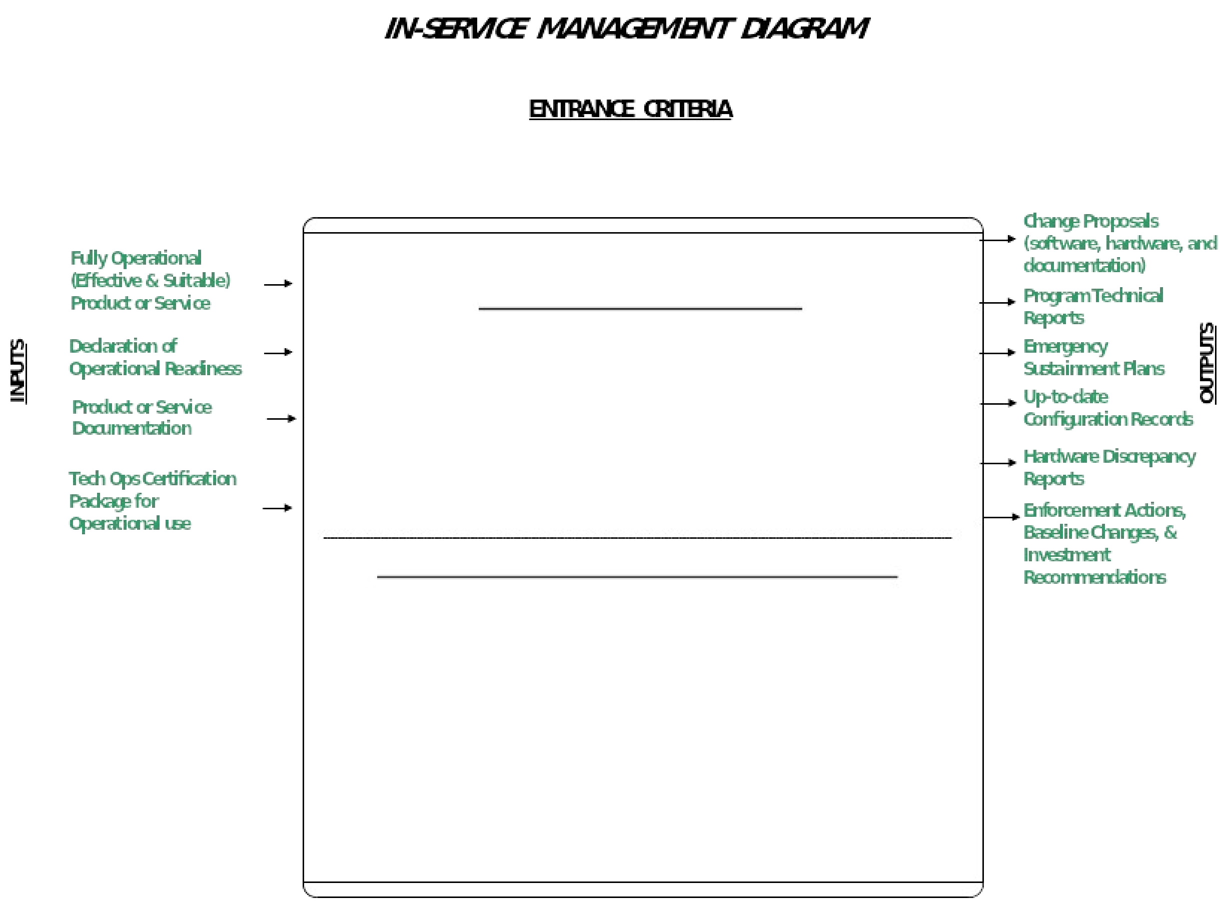


Figure 24-1. In-Service Management Inputs and Outputs

Solution Implementation Activities

The activities in this process include the following:

- Deliver ATC Products or Business Services
- Verify and Validate Key Work Products
- Sustain Services Within Baseline Values
- Perform Operational Analysis
- Maintain the System
- Manage Risk
- Maintain Product or Service Documentation

These activities are described below.

Deliver Air Traffic Control (ATC) or Business Services

The delivery of services is provided using infrastructure, procedures, personnel, and other assets as assigned and funded.

Systems Engineering Role

N/A

Activity Inputs

Fully Operational Product or Service
Declaration of Operational Readiness
Product or Service Documentation
Tech Ops Certification Package for Operational use

Activity Outputs

Program Technical Reports
Up-to-date Configuration Records
Hardware Discrepancy Reports

Potential SEM Chapter Reference

Configuration Management
Process Management

Verify and Validate Key Work Products

The service organization verifies and validates key work and in-service management products such as NAS change proposals and system support directives. Key work products that originated in other phases of the life cycle, but are modified during in-service management, are subject to verification and validation. Verification and validation activities support decisions to implement and deploy procedural and/or product improvements.

Systems Engineering Role
The systems engineer confirms that modified work products have met product requirements (Verification) and have solved the technical or operational shortfall (Validation).

Activity Inputs
Engineering change solution to an operational problem or shortfall

Activity Outputs
Fully verified and validated engineering change (software, hardware, and/or documentation)
Emergency sustainment plan
Up-to-date configuration records
Enforcement actions

Potential SEM Chapter Reference
Validation
Verification

Sustain Services Within Baseline Values

Management and engineering efforts throughout in-service management sustain and improve service delivery, correct deviations from cost and performance standards, and improve quality. These efforts include hardware and software modifications to solve latent or discovered technical problems, process changes to improve performance, planned block upgrades and product improvements, and sustainment actions that lower operating costs. It involves managing personnel, information systems, budget, logistics support, spare parts, technical resources, and other assigned assets. Management techniques include fiscal and workforce planning, contract award and administration, fiscal and program control, and process management to achieve cost, performance, and benefit objectives. All modifications to fielded assets must be in accordance with the enterprise architecture. If a planned modification requires a change to the architecture, appropriate amendments and products must be developed and approved.

Systems Engineering Role
The systems engineer analyzes, recommends, and implements proposed software/hardware modifications that enhance the system by accomplishing one or more of the following: address identified issues, process changes to improve performance, upgrade software/hardware, and perform sustainment actions that lower operating costs.

Activity Inputs

Service shortfall
Program technical reports
Hardware discrepancy reports

Activity Outputs
Change proposals (software, hardware, and/or documentation)
Up-to-date configuration records
Enforcement actions
Baseline changes
Investment recommendations

Potential SEM Chapter Reference
Integrated Technical Planning
Integrity of Analyses
Risk Management
Configuration Management
Life Cycle Engineering
Process Management

Perform Operational Analysis

Periodic operational analysis of fielded assets helps determine whether performance and customer expectations are being achieved. This type of evaluation continues throughout in-service management helping identify performance concerns, cost-of-ownership, and adverse support trends. The information gathered helps evaluate systemic problems and forms the basis of whether to continue to sustain existing assets or to recommend new investments to solve systemic operational problems in the service environment.

In-Service decision making needs to take two factors into account: (1) assessing the timing for technology insertion or capability replacement, and (2) determining whether modifications or improvements are feasible within the approved sustainment baseline funding. If an engineering change to the system within the sustainment funding is unable to be supported, then the shortfall is addressed via the standard AMS Life Cycle phases. If the effort to modify and/or optimize system performance is within the scope of sustaining funds, then the various SE elements are employed as in the Solution Implementation phase but on a lesser scale. The specific SE process application and associated level of effort depend on the scope of the upgrade.

Systems Engineering Role

The systems engineer evaluates current and past operational data of the fielded asset to determine if expected performance and customer expectations have been attained.

Activity Inputs
Operational risks or shortfalls identified in the Post-Implementation Review
Operational and performance data

Activity Outputs
Operational or maintenance issues or shortfalls requiring corrective action
Engineering recommendations for correcting operational or performance issues

Potential SEM Chapter Reference
Risk Management
Decision Analysis
Reliability, Maintainability and Availability

Maintain the Operational Asset
Modifications to fielded assets must be accompanied by associated support infrastructure changes such as training, documentation, spare parts, and relevant engineering support. This includes training for personnel who directly operate, maintain, and/or support the asset.

Systems Engineering Role
The systems engineer maintains the numerous components tied to a modification of fielded assets. This would include, for example, procedures, training, and support for a hardware/software modification.

Activity Inputs
Fully operational product or service
Product or service documentation

Activity Outputs
Up-to-date configuration records
System/Service Manuals
System/Service training Packages and Course
Operating procedures

Potential SEM Chapter Reference
Life Cycle Engineering

Data Management

Interdependencies

Integrated Technical Planning
Requirements Management
Interface Management
Risk Management
Configuration Management
Information Management
Technical Assessment
Validation
Deployment and Transition
Human Factors
Information Security
System Safety
Hazardous Materials/Environmental Engineering

References and Tools

Reference or Tool	Description
FAA Acquisition Management System Toolset (FAST) http://fast.faa.gov	AMS Policy establishes all requirements for acquisition management over the full life cycle at FAA. Specifically, it lists requirements for the activities that must be completed during in-service management, the outputs and products of each activity, the responsible agent or agents, and who approves each output.

25 – Special Considerations for System of Systems

Introduction

As FAA develops the Next Generation Air Transportation System (NextGen), the National Airspace System (NAS) is evolving into a System of Systems (SoS). To address this entity known as an SoS, the systems engineer needs to know what one is and what challenges it brings. Unfortunately, SoS is a relatively young field[1] with few established system of systems engineering (SoSE) processes. Although the Department of Defense has been working on developing an SoSE[2], the topic is still under research. With that in mind, this chapter provides a definition of SoS, a means to identify an SoS apart from other types of systems, and presents a list of known challenges. In addition, the chapter includes some suggestions for SoSE and integration of an SoS, based on existing research.

At a minimum, an SoS is fundamentally a system, as its name suggests, that exists as an amalgamation of other autonomous systems. However, there are two different mainstream viewpoints on SoSs[3,4]. On one hand, an SoS may be a matter of perspective where every system can be considered part of a larger system[5]. In this case, there is nothing exceptional about an SoS and, consequently, no reason to focus on SoS apart from traditional systems. Accepting this view implies no conceptual difference between the NAS and any of its constituent systems. On the other hand, an SoS is a distinct entity with a unique set of characteristics and traits. Given this view, there is good reason to call out NextGen as an SoS since it requires special considerations. This chapter accepts an SoS as a unique type of system with a defined user need, resources designated to address the need, and an agency responsibility to address this need.

Objective

The main objective of special considerations for System of Systems is to provide guidance for the identification of an SoS and recognize the challenges associated with an SoS.

Identifying a System of Systems

According to the current research on SoS, “Most agree that a system of systems arises when a set of needs are met through a combination of several systems”[6]. An SoS is a compilation of distributed, complex

component systems[7], or multiple, independent systems that interact for the purpose of a global goal[8].

An SoS is a collection of independent systems that work together to achieve some common purpose[1,9,10]. There can also be distinguishing characteristics, such as physically distributed systems, functionality that emerges from the connections between systems, and system heterogeneity[11]. An SoS evolves slowly over time and is more complex than developing stand-alone systems[12]. Heterogeneous systems within an SoS are integrated for the purpose of working effectively together[13]. The union of unique, individual systems forms a new SoS with a different function than any one of the individual systems had[14], and the various systems within an SoS can achieve results together that they could not do alone[15,16].

An often cited depiction of SoSs describes a collection of component systems with two additional properties. Each component system must have its own purpose independent of the other systems, and the component systems must maintain their independence [17]. Expanding on that description, Boardman and Sauser[18] review 41 papers on SoSs to extract commonalities from the definitions. They divide the various traits into common descriptive characteristics, which define an SoS as well as differentiate it from other systems. These five "essential characteristics" are Autonomy, Diversity, Belonging, sufficiently dynamic Connectivity, and Emergence[3,18,19]. Autonomy is the ability to complete one's own goals, and diversity indicates the goals of each system within the SoS differ. Belonging is the contribution to the goal of the SoS in exchange for advancing the system's goals. Connectivity implies dynamic connectivity where the systems are interconnected in a robust manner[3,4] The final characteristic of emergence has been postulated for SoS but has not been adequately defined to identify uniquely in some SoS. It indicates the presence of some behavior or feature that arises within the SoS but cannot be traced to any one constituent system. Since any system is said to be more than the sum of its parts, further research needs to specify how emergence differs, if at all, from a system and a SoS.

In summary, an SoS is a type of system comprising a diverse set of constituent systems with unique contributions. An SoS differs from a traditional system in that an SoS consists of multiple, diverse, autonomous systems, while the constituents of a traditional system are not autonomous[3]. An autonomous system is one that can meet its overall system goals[20]. For example, an aircraft is an autonomous system since it meets its goals of aerial transportation, but a propulsion system is not autonomous since it only contributes to the aircraft's goals. The constituent systems must be interconnected in such a way that allows systems to join and leave the SoS as needed.

An SoS has a set of goals unique from the goals of its constituent systems. The constituent systems must be autonomous systems in what they do. They must contribute towards the goals of the overall SoS and may help other systems achieve their goals in return for help towards their own goals[20]. The resultant complexity of the interconnected systems produces emergent features, in other words behavior that cannot be traced to any constituent system. It is possible, however, for both traditional systems and SoSs to be complex. The term complexity is often used frivolously to indicate difficult or complicated[21]. For the purposes of this chapter, complexity (as it applies to any type of system) occurs when emergent behavior cannot be predicted from its individual parts[22]. Therefore, complexity prevents an understanding of the whole based on the parts, or constituent systems, alone.

Examining the NAS reveals these SoS characteristics. The NAS is composed of many diverse constituent systems, such as ERAM, WMSCR, ADS-B, etc. Any of these constituent systems could function on its own to accomplish its particular goals, provided it receives the needed inputs. The systems within the NAS are connected. As the NAS evolves into NextGen, this connectivity should become more dynamic with systems such as the System Wide Information Management (SWIM). Perhaps less with previous incarnations of the NAS, NextGen systems will interoperate in such a way that multiple systems function together for a common purpose, such as ADS-B.

Just as there are many types of systems, there are potentially multiple types of SoS. These five types of SoS may not be exhaustive but they do give an idea as to how SoSs may differ.

- A **virtual** SoS is a collection of component systems, which are not engineered or acquired to be part of a SoS, but develop the SoS characteristics when connected[23].
- A **collaborative** SoS consists of component systems that willingly interact to fulfill the collective goal[24]. In a virtual a collaborative SoS, the integration is relatively straightforward as the systems practically integrate themselves.
- A **chaotic** SoS has no agreed-upon goal and the constituent systems interact as they see fit. The random interactions cause unpredictable behavior[23].
- An **acknowledged** SoS has recognized overall goals but the constituent systems maintain their independence[24]. An example of this type of SoS is a federated system, where there is a central program office but the constituent systems participate via documented agreements.

- A **dedicated** SoS is built and integrated for a specific purpose[24]. They are consciously designed and engineered from the beginning to be an SoS[23].

An example of a virtual SoS could be the early days of the NAS. The NAS was not originally planned but emerged with the development of air traffic control systems. However, NextGen is planned to be an SoS, which would make it a dedicated SoS. Although these differences exist, all SoSs share some common characteristics, by definition, and by challenges.

Challenges of a System of Systems

An SoS is a type of system, and any engineered system has its share of obstacles. However, an SoS has additional challenges. These difficulties include the following:

- Autonomy of systems causes each system to operate independently, for the most part[15]
- Requirements regarding the overall SoS functionality are likely to be ambiguous[15]
- Interaction of systems grows exponentially as constituent systems are added to the SoS[15]
- Interfaces conflict and the documentation becomes poorly defined as the interaction of systems grows, and so does the importance of interface management.
- Management of each constituent system overshadows engineering efforts for the SoS[15]
- Fuzzy boundaries within the SoS cause confusion[15]
- Diversity of SoS configurations cause management problems[15]
- SoSs evolve over time and therefore engineering is never finished[17]
- Interoperability of constituent systems causes changes in one system to have unexpected impact on other systems[2]
- Functionality emerges from the connections between constituent systems[11]
- Test and validation is distributed and federated, which complicates testing[2]

This list of challenges may not be inclusive as the emergent nature of an SoS can cause any number of challenges. Many of these challenges are already present when dealing with the NAS and more should be expected with NextGen. For example, one obvious challenge when dealing with any constituent system in an SoS is risk management. Due to the interconnected

nature of the systems, a change to one system may ripple through other systems. However, risk management traditionally focuses on the system of interest and generally lacks authority to mitigate risks outside of its domain. Challenges such as this one must be addressed as NextGen develops. In any case, this list gives the systems engineer an idea of the difficulties that one may face when engineering aspects of NextGen.

System of Systems Engineering (SoSE)

Most, if not all, aspects of classical systems engineering apply in some part to SoS, but classical systems engineering is insufficient to handle all aspects of these complex systems. Since SoSs are different than traditional systems, appropriate engineering techniques need to address them. One of the main differences is the need to focus on the relationships among the constituent systems in addition to the functions of each system. From General Systems Theory, “You cannot sum up the behaviour of the whole from the isolated parts, and you have to take into account the relation between the various subordinated systems and systems which are super-ordinated to them in order to understand the behaviour of the parts.”[25] This action of considering the whole and the interaction of parts constitutes the systems approach.

In an SoS, the interrelationships caused by the dynamic connections between constituent systems produce many emergent features[26]. A systems approach starts to address these interconnections by considering the gaps between systems in addition to the systems themselves. The systems approach can be defined as, “an approach to a problem which takes a broad view, which tries to take all aspects into account, which concentrates on interaction between the different parts of the problem”[27]. Yet, the systems approach does not abandon reductionism while emphasizing a more holistic view. Reductionism is a scientific approach that focuses on reducing things to the interactions of the parts, or to more fundamental things. On the other hand, holism considers a system or thing as a whole and may best be summarized as the belief that the whole is more than the sum of the parts. A true systems approach attempts to understand the nature of complex systems by reducing them to the interactions of their parts, i.e, reductionism, while considering the system as a whole, i.e., holism.

Another emergent feature requiring a system approach is the adaptive nature of an SoS. Constituent systems may not integrate in the traditional manner but rather collaborate as needed. Such constituent systems must be designed and managed to optimize the chance for collaboration. Combinations of systems operating together within the SoS contribute to the overall capabilities and the performance and behavior of the SoS can have stronger dependencies than expected between the constituent systems. The

individual systems may not have been designed for this level of dependency in their usual course of operation, and SoS capabilities may depend more strongly on emergent behaviors than is usually expected from a single system. As with emergent behaviors of single systems, these behaviors may either improve performance or degrade it.

SoSE typically involves multiple system life cycles that are not necessarily part of a single acquisition program. Rather, the SoS may comprise legacy systems, developmental systems in acquisition programs, technology insertion, life extension programs, and systems related to other initiatives. The acquisition of SoS capability generally will not be driven solely by a single organization but rather may involve multiple program offices and support communities[2]. Consequently, lifecycle engineering has a different challenge of managing an architecture that is constantly changing as the SoS evolves. The lifecycle engineers assigned to each constituent system must communicate often in order to be prepared for changes imposed by other systems. Since the SoS evolves with new systems coming on line as old ones are decommissioned, the lifecycle engineering aspect of SoSE must pay greater attention to the disposal process.

Integration in System of Systems

In general, it is more difficult to test and assemble an SoS than a single system due to the diverse, autonomous constituent systems. At a minimum, testing and validation can be expected to be largely distributed[2]. Research is ongoing to determine appropriate testing and validation methods. Aspects such as security, safety, assurance, reliability, and net-centricity need to be reassessed for the SoS. While the constituent systems may meet all assurance requirements, the networking of these systems into an SoS may introduce new vulnerabilities. In addition, the communication system should be explicitly evaluated for security, safety, reliability, and assurance. An SoSE challenge is to leverage the functional and performance capabilities of the constituent systems so as to achieve the desired SoS capability.

The performance of an SoS is dependent not only on the performance of the individual constituent systems but also on their evolutionary state. For the SoS to function, its constituent systems must be integrated to achieve physical connectivity, and interoperability at all levels, including physical, logical, semantic, and syntactic interoperability. Interoperability allows the necessary connectivity across the SoS to be defined. The boundary of any SoS can be relatively ambiguous because of the dynamic operational focus, multi-mission, and often ad hoc nature of the operational environment of the SoS. In this type of environment, there is a potential for ad hoc coupling across both organizational and systems boundaries in support of the

dependencies created. Therefore, in order to use systems successfully, in an SoS context, the protocols used to support the specification of interfaces should be ubiquitous. The interfaces are key convergence points for SoS, and there may be no opportunity for changes to the interfaces without major impact to the entire SoS. The development and management of an SoS architecture through the evolution of an SoS is the mechanism used to document and share information among constituent systems to support integration[2].

Understanding the constituent system characteristics, functionality, and interfaces is essential to integrating systems into an SoS. Some constituent systems may have interfaces that are changeable without major impact, but others may be prohibitively expensive to modify or may be based on an existing standard[2]. It is possible that many interfaces are not well-defined or potentially conflicting with other systems[15]. Hence SoSE must address the interfaces and interactions of systems during integration. Other than stressing the importance of diligence, little guidance is currently available for any one successful process.

Differences between a Traditional System and an SoS

Traditional System	System of Systems
Overall system is autonomous but its parts are not	Overall SoS is autonomous as well as its constituent systems
Parts of a system collaborate only to the extent they are designed	Constituent systems collaborate as needed to help each other reach their goals
Parts of a system are statically connected	Constituent systems may be dynamically connected, joining and separating from the SoS as needed
Each system is unique	SoS is composed of a diversity of constituent systems
A system is more than the sum of its parts but may not necessarily be complex	An SoS exhibits emergent functionality that cannot be traced to any particular constituent system and may be the result of the dynamic connectivity of the constituent system.
Service unit systems such as ERAM, ADS-B, WMSCR, etc.	Current and future NAS (ie. NextGen)

Interdependencies

Life Cycle Engineering
Integration

References

1. Shenhar, A.J. & Sauser, B. Systems engineering management: The multidisciplinary discipline. *Handbook of systems engineering and management* 117-154 (2009).
2. ODUSD(A&T)SSE *Systems engineering guide for systems of systems*. (Office of the Deputy Under Secretary of Defense for Acquisition and Technology: Washington, DC, 2008).at <http://www.acq.osd.mil/sse/docs/SE-Guide-for-SoS.pdf>
3. Baldwin, W.C., Felder, W.N. & Sauser, B.J. Taxonomy of increasingly complex systems. *Int. J. Ind. Syst. Eng.* **9**, 298-316 (2011).
4. Baldwin, W.C. & Sauser, B. Modeling the characteristics of system of systems. *2009 IEEE International Conference on System of Systems Engineering (SoSE)* (2009).
5. Ackoff, R.L. Towards a system of systems concept. *Manag. Sci.* **17**, 661-671 (1971).
6. Exton Jr., W. *The age of systems: The human dilemma*. (American Management Association, Inc.: United States of America, 1972).
7. Phillips, D.C. The methodological basis of systems theory. *Academy of Management Journal* **15**, 469-477 (1972).
8. Carney, D., Fisher, D. & Place, P. *Topics in interoperability: System of systems evolution*. (Carnegie Mellon University/Software Engineering Institute: Pittsburgh, PA, 2005).at <http://www.sei.cmu.edu/publications/documents/05.reports/05tn002.html>
9. Manthorpe, W.H.J. The emerging joint system-of-systems: A systems engineering challenge and opportunity for APL. *Johns Hopkins APL Technical Digest* **17**, 305-310 (1996).
10. DeLaurentis, D.A. & Crossley, W.A. A taxonomy-based perspective for systems of systems design methods. *Systems, Man and Cybernetics, 2005 IEEE International Conference on* **1**, 86-91 (2005).
11. Kotov, V. *Systems-of-systems as communicating structures*. (Hewlett Packard Computer Systems Laboratory: 1997).
12. Crossley, W.A. *System of systems: An introduction of Purdue University Schools of Engineering's signature area*. (School of Aeronautics and Astronautics, Purdue University: 2004).at <http://esd.mit.edu/symposium/pdfs/papers/crossley.pdf>
13. Shenhar, A.J. One size does not fit all projects: Exploring classical contingency domains. *Manag. Sci.* **47**, 394-414 (2001).

14. Shenhar, A.J. & Bonen, Z. The new taxonomy of systems: toward an adaptive systems engineering framework. *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans* **27**, 137-145 (1997).
15. DeLaurentis, D.A. & Callaway, R.K. System-of-systems perspective for public policy decisions. *Rev. Pol. Res.* **21**, 829-837 (2004).
16. Carlock, P.G. & Fenton, R.E. System of systems (SoS) enterprise systems engineering for information-intensive organizations. *Systems Engineering* **4**, 242-261 (2001).
17. Carlock, P.G., Decker, S.C. & Fenton, R.E. Agency-level systems engineering for “systems of systems.”*Systems and Information Technology Review Journal* **7**, 99-110 (1999).
18. Kang, T. & Mavris, D.N. *A system-of-systems approach for application to large-scale transportation problems*. (INCOSE: 2005).at <http://www.incose.org/practice/techactivities/wg/sysarch/>
19. INCOSE *INCOSE systems engineering handbook: A guide for system life cycle processes and activities*. (International Council on Systems Engineering: Seattle, WA, 2010).
20. Krygiel, A. *Behind the wizard’s curtain*. (Institute for National Strategic Studies: Washington, DC, 1999).at <http://www.dodccrp.org/html4/books_downloads.html>
21. Maier, M.W. Architecting principles for system-of-systems. *Syst. Eng.* **1**, 267-284 (1998).
22. Boardman, J. & Sauser, B. System of Systems - the meaning of of. *Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering* 118-123 (2006).doi:10.1109/SYSOSE.2006.1652284
23. Gorod, A., Sauser, B. & Boardman, J. System-of-systems engineering management: A review of modern history and a path forward. *IEEE Syst. J.* **2**, 484-499 (2008).
24. Baldwin, W.C., Ben-Zvi, T. & Sauser, B.J. Formation of collaborative system of systems through belonging choice mechanisms. *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans* **Early Access**, 1-9 (2011).
25. Biggiero, L. Sources of complexity in human systems. *Nonlinear Dynamics, Psychology, and Life Sciences* **5**, 3-19 (2001).
26. Calvano, C.N. & John, P. Systems engineering in the age of complexity. *Syst. Eng.* **7**, 25-34 (2004).
27. Gideon, J.M., Dagli, C.H. & Miller, A. Taxonomy of systems-of-systems. *Proceedings CSER 2005* (2005).
28. Dahmann, J.S., Rebovich Jr, G. & Lane, J.A. Systems engineering for capabilities. *CrossTalk* **21**, 4-9 (2008).
29. von Bertalanffy, L. An outline of general systems theory. *British Journal for the Philosophy of Science* **1**, 139-164 (1950).
30. Schelling, T. *Micromotives and macrobehavior*. (W.W. Norton & Co.: New York, 1978).

31. Checkland, P. *Systems thinking, systems practice: Includes a 30-year retrospective*. (John Wiley & Sons: Chichester, England, 1999).

This page intentionally left blank.

26 – Reliability, Maintainability, and Availability (RMA) Engineering

Introduction

This section provides guidance to facilitate, manage, and coordinate Reliability, Maintainability, and Availability (RMA) efforts, to ensure operationally acceptable RMA characteristics in fielded systems. SEM RMA Engineering is based on the FAA RMA Handbook [FAA-HDBK-006A] which includes the rationale for the RMA Engineering approach and explains the process in more detail. Section 3 of the handbook includes definitions of RMA engineering terms and parameters and provides background and context for the RMA Engineering discussions that follow. Handbook Appendices provide sample requirements and supporting analytical material.

The purpose of this section is to assist FAA Service Units and acquisition managers in the preparation of the RMA sections of procurement packages for major system acquisitions. The affected documents include System-Level Specifications (SLS), Statements of Work (SOWs), Information for Proposal Preparation (IFPP) documents, and associated Data Item Descriptions (DIDs).

Definition

RMA Engineering applies engineering and management principles, criteria, and techniques to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system life cycle.

Reliability

Reliability is the ability of a system to perform as designed in an operational environment over time without failure. System reliability is commonly measured by Failure Rate and Mean Time between Failure (MTBF).

$$\text{Failure Rate, } (\lambda) = \frac{\text{Number of failures}}{\text{Total operating hours}}$$

Failure rate (λ) represents the instantaneous failure rate, or the number of times the event is expected to happen in a given period of time. Mean Time between Failures is represented by

the symbol Theta (θ); is the Mean Life, or the average lifetimes of all items under consideration.

$$\text{MTBF}, \theta = 1/\lambda = \frac{\text{Total operating hours}}{\text{Number of failures}}$$

Most FAA specifications for repairable or replaceable systems use Mean Time between Failures (MTBF). FAA's primary goal is safety, and increasing systems reliability is vital to the support of this goal. Systems reliability then supports Maintainability and Supportability, reducing operational costs and maintaining safety goals.

There are essentially two ways to accomplish this goal: Start with designing High Reliability systems, or Optimize logistics resources to allow decreased Maintainability and Supportability. Reliability and Maintainability are some of the design parameters that must be considered. These two parameters are often trade-off in other to meet a higher-level requirement such as Availability. Refer to FAA handbook FAA-HDBK-006A, January 7, 2008 for more detail information.

Maintainability
Maintainability is measured by an item's ability to be retained in a specified condition through scheduled maintenance, or restored to a specified condition through proper repair.

Maintainability evolves from a series of statements and illustrations defining the input criteria to which the system should be designed. It evolves into a description of the planned levels of maintenance, major functions accomplished at each level, organizational responsibilities, basic support policies, design criteria associated with the support elements such examples include; built-in-test versus external testing, and personnel skill-level requirements, effectiveness criteria and anticipated maintenance environment requirements. Preliminary maintenance concept is developed during conceptual system design, and thereafter continuously updated in order to provide the desired influence on the mainstream system design and development. This system maintenance concept should address the question of "How will the system be supported, where, and for how long?"

Mean Time to Repair (MTTR) is a basic measure of maintainability. The MTTR is an inherent system design characteristic. Traditionally, this characteristic represents an average of the times needed to diagnose, remove, and replace failed hardware components. In effect, it is a measure of how easy it is to access malfunctioning equipment's failed components in combination with the effectiveness of diagnostics and built-in test equipment to detect and isolate the failure and the actions needed to return the equipment to service. The MTTR for a piece of equipment is related to the reliability (failure rate) of

the various components comprising the equipment and the time to replace each of them.

For information systems, the Mean Time to Restore Service (MTTRS) is often used. It includes times for software reloading and system restart times in addition to the equipment repair time.

Availability

Availability is the probability that a system or part of a system may be operational during any randomly selected instant of time or, alternatively, the fraction of the total available operating time that the system or part is operational. Measured as a probability, availability may be defined in several ways, which allows a variety of issues to be addressed appropriately, including:

Inherent Availability (A_i) – The maximum theoretical availability within the capabilities of the system or part. Computations of this construct consider only hardware elements and they assume perfect failure coverage, an ideal support environment, and no software or power failures. Scheduled downtime is not included in the Inherent Availability measure. A_i is an inherent design characteristic of a system that is independent of how the system is actually operated and maintained in a real-world environment.

Equipment and Service Availability (A_{es}) – Includes all sources of down time associated with unscheduled outages, including logistics and administrative delays, but excludes scheduled downtime. A_{es} is an operational performance measure for deployed systems and is monitored by the National Airspace Reporting System (NAPRS) for all reportable facilities and services.

Operational Availability (A_{op}) – The availability including *all* sources of downtime, both scheduled and unscheduled. A_{op} is an operational measure for deployed systems that is monitored by NAPRS.

Relationship between Reliability, Maintainability, and Availability

Inherent Availability can be derived from the reliability and maintainability according the formula:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Availability can also be used as an operational performance metric for deployed systems by dividing the total time that the system or service is available in an interval by the total time in the interval. Operational availability combines the reliability performance of the operational system with the performance of maintenance personnel responsible for restoring service (following an interruption) into a single performance measure.

Availability can be useful as:

- A high-level planning tool for assessing architecture alternatives
- A tool for performing reliability and maintainability tradeoff analyses for logistics and Life Cycle Cost studies
- An operational performance metric for deployed systems

Availability is <u>not</u> appropriate for inclusion in contractual requirements as a primary specification for highly reliable systems. Availability is a gross oversimplification when applied to complex, software-intensive, fault-tolerant, information systems built from commercial, off-the-shelf hardware. Reasons why availability is not appropriate as the primary RMA requirement for modern digital systems include:

- **Availability implies that reliability and maintainability can be traded off.** Consider two automation systems, one having a predicted restart time of 3 minutes and a predicted MTBF of 5000 hours, and the other having a predicted 3 hour restart time and a predicted MTBF of 34 years. Both have a predicted availability of .99999, but the operational impact of failures would be vastly different. Moreover, while restart times are readily verifiable, MTBF predictions of 34 years are not credible and cannot be verified. Trading off actual restart times with problematic reliability predictions is unacceptable.
- **Availability cannot be predicted with enough accuracy to be useful.** Although the inherent availability of the hardware architecture can be predicted by straightforward combinatorial probability models, the primary determinate of the availability of software-intensive fault-tolerant systems is the effectiveness of the fault detection and recovery software. Since this effectiveness is dependent upon the effects of undiscovered defects in the software, it is virtually impossible to predict availability with any credibility before the software has been developed.
- **Contractual compliance with availability requirements cannot be verified.** It is impractical to conduct a statistically valid demonstration of the availability required by NAS systems. To achieve a statistically valid result, the duration of the availability demonstration test would have to exceed the expected lifetime of the system. Moreover, it is virtually impossible to conduct a static demonstration of the system availability; problems will be continuously found and corrected and decisions will need to be made concerning which failures are relevant and how much of the resulting downtime is to be included in the availability calculation. Many of these factors are beyond the contractor's ability to control.

For these reasons, availability does not meet the SEM guidelines for good requirements. [See FAA-HDBK-006A Section 5.2.3 and Chapter 12 (Functional and Performance Allocation Process).]

The primary causes of unscheduled service interruptions in modern information systems are latent software defects and excessive maintenance delays in restoring or replacing failed spare equipments, not hardware failures. Restoration times may be more dependent on computer restart times than hardware replacement times.

Objective

Unlike most government agencies, where safety is simply a design constraint to attempt to prevent unintended consequences that could cause injury to persons or the environment, FAA's *primary* mission is safety. For this reason, RMA Engineering in FAA is closely related to both system safety engineering and risk management. Safety and efficiency are the primary considerations in the RMA Handbook's top-down allocation of availability requirements to FAA systems.

The purpose of the RMA section of the SEM is not to tell contractors how to build reliable hardware, but to provide guidance to FAA RMA engineers and acquisition managers on how to address many issues. Among these are: architectural issues, system-level RMA specifications, procurement package preparation, contractor proposal evaluations, design development monitoring, and the establishment of design validation and reliability growth criteria. Reliability, Maintainability, and Availability directly impact both operational capability and life cycle costs and, therefore, are important considerations in any systems engineering effort.

The RMA characteristics of FAA systems are uniquely important because they can directly affect the ability to perform the Agency's mission. Interruptions of critical services provided to air traffic specialists can adversely affect the efficiency of air traffic movement as controllers invoke manual procedures to maintain safety. However, during the transition interval from normal capacity operation to reduced capacity operation, safety hazards can exist as controllers increase separation and clear out the airspace until a steady state is reached. Figure 26-1 illustrates the transition to reduced capacity and the hazard interval during the transition. The triangle illustrates the interval in which safety hazards may occur. In most cases, this interval is non-existent or negligible and the only issue is the effect of the interruption on efficiency. Some interruptions may have only nominal impacts nationwide, while others may result in critical, nationwide disruption of service, but in neither case is safety affected. An example of an interruption with a potentially critical effect on efficiency but negligible effect on safety is the loss of flight data processing capability.

On the other hand, loss of surveillance data or voice communications can result in a critical safety hazard until controllers are able to reduce traffic density and increase separation. Once a service has been identified as critical to providing safe separation of aircraft, an independent backup for the service must be provided to reduce the risk to acceptable levels.

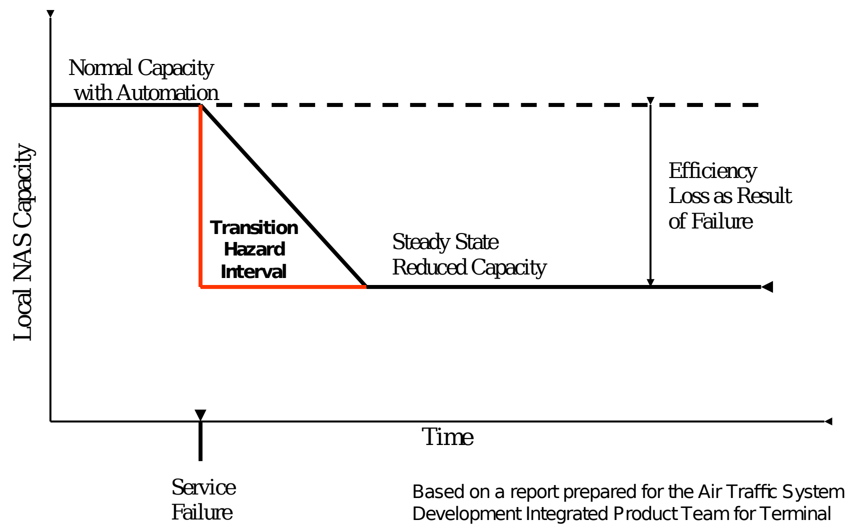


Figure 26-1. Effect of Service Interruptions on NAS Capacity

RMA Inputs

Inputs to the RMA Engineering process include:

- FAA Policy and Standards
- NAS Enterprise Architecture
- NAS Requirements
- Systems Engineering Management Plan (SEMP)
- Program Requirements
- Functional and Performance Allocation
- Physical Architecture
- Contractor Technical Interchange Meetings and Briefings
- Contractor Data Item Deliverables

RMA for FAA Systems

For the purposes of RMA, there are at least three categories of FAA systems: Information Systems, Remote/Distributed Systems, and Infrastructure Systems. Each category has different attributes that dictate unique treatment when specifying RMA.

Information Systems

These are characterized and allocated by the NAS-Level RMA requirements. Information systems involve software-intensive air traffic control automation and communications capabilities. They have stringent availability requirements and, as a consequence of the large amounts of custom software that must be developed for them, entail significant cost and schedule risks. These programs provide the most critical operational services and have the most visibility. For these reasons, it is appropriate that they be given the most attention.

Remote/Distributed Systems

These are characterized by equipments such as sensors that “fan-in” to an information subsystem or services that “fan-out” from an information subsystem to a number of display workstations. These subsystems achieve the necessary overall availability through their reliance upon techniques such as diversity and overlapping coverage tailored to meet specific regional considerations. The subsystems are very robust because failures of individual elements only *degrade* the overall capability of the subsystem. It is not appropriate to attempt a “top-down” allocation of availability to these subsystems. Availability is a binary “up or down” measure that does not appropriately characterize subsystems that consist of multiple independent elements. To allocate availability to these elements requires making arbitrary “r of n” failure definitions, *e.g.*, 49 of 50 radars must be up for the surveillance subsystem to be up. If only 48 radars are operational, the entire surveillance subsystem is considered to be down. This does not reflect operational reality and can lead to unrealistic availability allocations. The availability requirements for the individual elements comprising these subsystems are best determined by life-cycle cost considerations, and acquisition managers’ knowledge of achievable levels of reliability for the particular element in question. The overall operational suitability of the subsystem is best achieved by the judgment of subject matter experts in determining the number and placement of subsystem elements, not by an artificial and arbitrary mathematical allocation.

Infrastructure Systems

The infrastructure systems category refers to systems such as power systems, or heating, ventilation, and air conditioning (HVAC) systems that are required to support the equipment comprising the Service Threads. These systems typically violate the independent failure assumption underlying RMA calculations, as they can directly cause failures in the systems they support. Therefore, top-down allocations of availability requirements are not appropriate for these systems. Instead, FAA needs to develop a well-defined set of standard configurations that are consistent with the availability requirements of the Service Threads they support. The

Service Threads are based on the National Airspace Performance Reporting System (NAPRS) services defined in FAA Order 6040.15. They represent “end-user” services delivered to air traffic specialists, and are essentially a reliability block diagram containing all of the “sensor to glass” equipments required to provide the service to the end-user.

NAS-Level RMA requirements are provided to satisfy the following objectives:

- Provide a bridge between NAS-Level user needs and System-Level Specifications.
- Establish a common framework upon which to justify future additions and deletions of requirements.
- Provide uniformity and consistency of requirements across procured systems, promoting common understanding among the specifying engineers and the development contractors.
- Establish and maintain a baseline for validation and improvement of the RMA characteristics of fielded systems.

RMA Process Tasks

RMA Engineering follows the specific process tasks described in Figure 26-1, below.

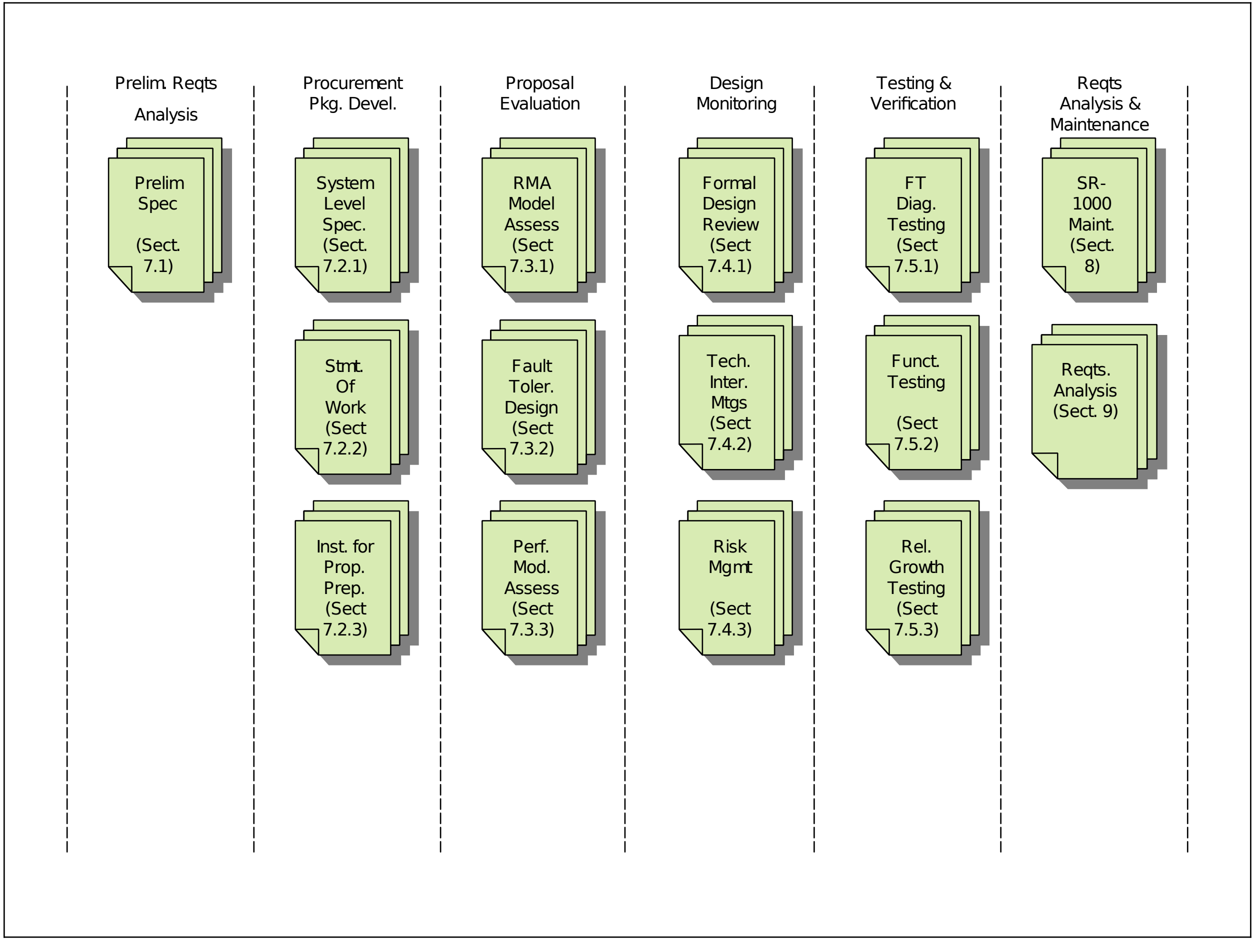


Figure 26-1. RMA Process Tasks

Figure 26-1 depicts the relationship of the six RMA process tasks. The process task flow is from left to right and follows the acquisition process flow. Each step in a process task is keyed to the section of the RMA Handbook that describes the document to be produced.

Task 1: Preliminary Requirements Analysis

The primary objective of the preliminary requirements analysis task is to build a “bridge” between NAS-Level requirements and the procurement specifications for the tangible systems that will implement the NAS requirements. The Service Threads are essentially a reliability block diagram containing all of the “sensor to glass” equipments required to provide the service to the end-user.

The process of allocating the availability requirements associated with NAS architecture capabilities to Service Threads is maintain in the RMA Handbook. This allocation is update with the maintenance of the RMA Handbook, SEM, and requirements documents as the NAS evolves. The handbook describes the detailed methodology used to perform the Preliminary Requirements Analysis Task.[3] A traceability matrix specifies the relationship between the NAS architecture capabilities and the Service Threads. This matrix is a predecessor to the Operational Activity to Systems Function Traceability matrix (SV-5) in the NAS Enterprise Architecture Framework, where the NAS capabilities correspond to the Operational activities (OV-5) and the Service Threads are equivalent to the Systems Functions (SV-4).

Three criticality levels known as "Service Thread Loss Severity Categories (STLSCs):" are associated with the interruption of the service provided by a service thread with an allocated availability requirement established for each. Reliability and Maintainability requirements were established for the systems contained in a service thread, consistent with the allocated service thread availability.

The three STLSCs are:
Essential – Service Thread loss could be accommodated by reducing capacity without compromising safety, with only a localized impact on NAS efficiency. (A = .9999)
Efficiency-Critical – Service Thread loss could be accommodated by reducing capacity with economic impact on NAS efficiency without compromising safety, but the resulting effect might have a localized or system-wide impact (A = .99999)
Safety-Critical – Service Thread loss would present an unacceptable safety hazard during transition to reduced capacity operations. No single service thread can be permitted to provide a safety-critical service because there is no assurance that a single service thread can ever approach the required level of availability. Instead any proposed safety-critical thread *must* be decomposed into *two* independent service threads *each* having an availability of .99999[4].

Note that these Service Thread Loss Severity Categories (STLSCs) differ from the traditional criticalities associated with the NAS architecture capabilities. Critical failures are divided into two categories: those that pose a significant

[3] The process for allocating NAS-Level availability requirements to service threads is described in detail in [Section 7.1 of FAA-HDBK-006A, RMA Handbook

[4] The current NAS has no single safety-critical service threads, because each instance of a safety-critical service has a primary service thread as well as a backup service thread. However, in every case the backup service thread was only added after the achieved availability of the primary service thread was proven to be inadequate. This requirement is designed to prevent the establishment of unachievable availability requirements from the outset.

safety risk, and those that only affect system capacity. There is no STLSC corresponding to "routine" because a top-down allocation of availability would result in unacceptably low RMA requirements that could lead to unreliable systems with excessive maintenance costs.

Acquisition Managers need only to identify the service thread(s) associated with the system being acquired, identify the service thread with the highest service thread loss criticality, and apply the RMA requirements associated with that category to the system.

Most system acquisitions can be accommodated within the existing service thread structure, as they are replacing or improving components within an existing service thread. However, when systems providing an entirely new service are planned, it will be necessary to coordinate with System Engineering in defining new service threads.

In addition to the quantitative RMA requirements, the following RMA related characteristics need to be addressed:

- **Scheduled Downtime** – Although scheduled downtime is beyond the contractor's ability to control, it is still an important factor in ensuring the operational suitability of the system being acquired, and the need to accommodate scheduled downtime without operational disruption is a necessary factor in acquisition planning.
  Many NAS systems are not needed on a 24/7 basis; some airports restrict late operations, and some weather systems are only needed during periods of adverse weather. If projected downtime requirements can be accommodated without unduly disrupting Air Traffic Control operations by scheduling downtime during low traffic periods or when the system is not needed, then there is no impact.
  Conversely, if scheduled downtime cannot be accommodated without disrupting air traffic control operations, it is necessary to re-examine the approach being considered. It also may be necessary to add an independent backup system to supply the needed service while the primary system is unavailable.
- **Redundancy and Fault Tolerance Requirements** – The first determinant of the need for redundancy and fault tolerance is the required inherent availability of the hardware architecture. If the failure and repair rates of a single set of system elements cannot support the inherent availability requirements, redundancy and automatic fault detection and recovery mechanisms must be added. There must be an adequate number of hardware elements that, given their failure and repair rates, the combinatorial probability of running out of spares is consistent with the inherent availability requirements. When it is determined that redundancy and fault tolerance are required to meet RMA requirements, the performance characteristics of the fault

tolerance mechanisms such as switchover times and restart times need to be specified.

There are other reasons beyond the inherent availability of the hardware architecture that may dictate a need for redundancy and/or fault tolerance. Even if the system hardware can meet the inherent hardware availability, redundancy may be required to achieve the required recovery times and provide the capability to recover from software failures.

All Service Threads with a STLSC of “Efficiency-Critical” have rapid recovery time requirements because of the potentially severe consequences of lengthy service interruptions on the efficiency of NAS operations. These recovery time requirements will, in all probability, call for the use of redundancy and fault-tolerant techniques. The lengthy times associated with rebooting a computer to recover from software failures or “hangs” indicates a need for a standby computer that can rapidly take over from a failed computer.

[For a complete discussion of the allocation process and preliminary requirements analysis, see Sections 6 and 7.1 of FAA-HDBK-006A, RMA Handbook]

Task 2: Procurement Package Preparation

The primary objectives to be achieved in preparing the procurement package are as follows:

- To provide the specifications that define the RMA and fault tolerance requirements for the delivered system and form the basis of a binding contract between the successful offerer and the Government.
- To define the effort required of the contractor to provide the documentation, engineering, and testing needed to monitor the design and development effort, and to support risk management, design validation, and reliability growth testing activities.
- To provide guidance to prospective offerers concerning the content of the RMA sections of the technical proposal, including design descriptions and program management data required to facilitate the technical evaluation of the offerers’ fault-tolerant design approach, risk management, software fault avoidance and reliability growth programs.

The RMA-related parts of the procurement package include:

- **System Level Specification (SLS)** – The System-Level Specification serves as the contractual basis for defining the design characteristics and performance that are expected of the system. From the standpoint of fault tolerance and RMA characteristics, it is necessary to define the quantitative RMA and performance characteristics of the automatic

fault detection and recovery mechanisms. It is also necessary to define the operational requirements needed to permit FAA facilities personnel to perform real-time monitoring and control and manual recovery operations as well as diagnostic and support activities. In addition, the SLS RMA requirements should include parameters that specify the reliability growth required from the first system deployment to the last system deployment.

- **Statement of Work (SOW)** – The Statement of Work describes the RMA-related tasks required of the contractor to design, analyze, and monitor risk; implement fault avoidance programs; and prepare the documentation and engineering support required to provide Government oversight of the RMA, Monitor and Control function, fault-tolerant design effort, support fault-tolerance risk management, and conduct reliability growth testing.
- **Information for Proposal Preparation (IFPP)** – The Information for Proposal Preparation (IFPP) describes material that the Government expects to be included in the offerer's proposal.

Preparation of the RMA procurement package components is discussed in Section 7.2 of FAA-HDBK-006A, RMA Handbook.

Task 3: Proposal Evaluation

The following topics represent the key factors in evaluating each offerer's approach to developing a system that will meet the operational needs for reliability and availability:

- **Reliability Modeling and Assessment** – The evaluation of the offerer's inherent availability model is simple and straightforward. All that is required is to confirm that the model accurately represents the architecture and that the mathematical formulas are correct. The substantiation of the offerer's MTBF and MTTR values used as inputs to the model should be also reviewed and evaluated. Appendix B of the RMA Handbook provides tables and charts that can be used to check each offerer's RMA model.
- **Fault-Tolerant Design Evaluation** – The offerer's proposed design for automatic fault detection and recovery/redundancy management should be evaluated for its completeness and consistency. A critical factor in the evaluation is the substantiation of the design's compliance with the recovery time requirements. There are two key aspects of the fault-tolerant design. The first is the design of the software components that contain the protocols for health monitoring, fault detection, error recovery, and redundancy management. Equally important is the offerer's strategy for incorporating fault tolerance into the application software. Unless fault tolerance is embedded into the application software, the ability of the automatic recovery software to effectively mask software faults will be severely limited. The ability to

handle unwanted, unanticipated, or erroneous inputs and responses must be incorporated during the development of the application software.

- **Performance Modeling and Assessment** – An offerer should present a complete model of the predicted system loads, capacity, and response times. Government experts in performance modeling should evaluate these models. Fault tolerance evaluators should review the models in the following areas:
  - **Latency of fault tolerance protocols** – The ability to respond within the allocated response time is critical to the success of the fault tolerance design. It should be noted that, at the proposal stage, the level of the design may not be adequate to address this issue.
  - **System Monitoring Overhead and Response Times** – The offerer should provide predictions of the additional processor loading generated to support both the system monitoring performed by the M&C function as well as by the fault tolerance heartbeat protocols and error reporting functions. Both steady-state loads and peak loads generated during fault conditions should be considered.
  - **Relation to Overall System Capacity and Response Times** – The system should be sized with sufficient reserve capacity to accommodate peaks in the external workload without causing slowdowns in the processing of fault tolerance protocols. Adequate memory should be provided to avoid paging delays that are not included in the model predictions.

Fault Tree Analysis

Fault Tree Analysis (FTA) is a popular and productive risk identification tool. It provides a standardized discipline to evaluate and control hazards. The FTA process is used to solve a wide variety of problems ranging from safety to management issues.

This tool is used by engineers both prevent and resolve hazards, failures and risks. Both qualitative and quantitative methods are used to identify areas in a system that is most critical to safe operation. Either approach is effective. The output is a graphical presentation providing technical and administrative personnel with a map of "failure or hazard" paths.

The FTA is a graphical logic representation of fault events that may occur to a functional system. This logical analysis must be a functional representation of the system and must include all combinations of system fault events that can cause or contribute to the undesired event. Each contributing fault event should be further analyzed to determine the logical relationships of underlying fault events that may cause them. This tree of fault events is expanded until all "input" fault events are defined in terms of basic,

identifiable faults that may then be quantified for computation of probabilities, if desired. When the tree has been completed, it becomes a logic gate network of fault paths, both singular and multiple, containing combinations of events and conditions that include primary, secondary, and upstream inputs that may influence or command the hazardous mode.

Based on available data, probabilities of occurrences for each event can be assigned. Algebraic expressions can be formulated to determine the probability of the top level event occurring. This can be compared to acceptable thresholds and the necessity and direction of corrective action determined. The FTA shows the logical connections between failure events and the top level hazard or event. "Event," the terminology used, is an occurrence of any kind. Hazards and normal or abnormal system operations are examples.

The FTA's graphical format is superior to the tabular or matrix format in that the inter-relationships are obvious. The FTA graphic format is a good tool for the analyst not knowledgeable of the system being examined. The matrix format is still necessary for a hazard analysis to pick up severity, criticality, family tree, probability of event, cause of event, and other information. Being a top-down approach, in contrast to the fault hazard and FMECA (see below), the FTA may miss some non-obvious top-level hazards.

Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects
Criticality Analysis (FMECA).

The scope of this effort depends on system complexity, subsystem and external interfaces, and new design elements. The effort also impacts maintainability, testability, logistics, and safety analyses.

FMEA is an evaluation process for analyzing and assessing the potential failures in a system. The objective is to determine the effect of failures on system operation, identify the failures critical to operational success and personnel safety, and assess each potential failure according to the effects on other portions of the system. In general, these objectives are accomplished by itemizing and evaluating system composition and functions.

FMEA is a systematic method of identifying the failure modes of a system, a constituent piece, or function and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic, or mechanical). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode. The FMEA results may be used to support other analysis techniques, such as a fault tree analysis. Other techniques

that are occasionally used include the dependence diagram and Markov analysis.

Adding a criticality figure of merit is needed to generate the FMECA from the FMEA.

Assigning severity levels cannot be performed without first identifying the purpose of the FMECA.

See Section 7.3 of FAA-HDBK-006A, RMA Handbook for a more detailed discussion of these topics.

Task 4: Contractor Design Monitoring

The following activities should be conducted by FAA specialty engineers during system development:

- **Formal Design Reviews** – Formal design reviews are a contractual requirement. Although these reviews are often too large and formal to include a meaningful dialog with the contractor, they do present an opportunity to escalate technical issues to management's attention.
- **Technical Interchange Meetings** – The contractor's design progress should be reviewed in monthly Fault Tolerance TIMs. In addition to describing the design, the TIM should address the key timing parameters governing the operation of the fault tolerance protocols, the values allocated to the parameters, and the results of model predictions and or measurements made to substantiate the allocations.
- **FT Design Risk Management** – The objective of the fault tolerance risk management activities is to expose flaws in the design as early as possible, so that they can be corrected "off the critical path" without affecting the overall program cost and schedule. Typically, major acquisition programs place major emphasis on formal design reviews such as the System Requirements Review (SRR), the System Design Review (SDR) the Preliminary Design Review (PDR), and the Critical Design Review (CDR). After the CDR has been successfully completed, lists of Computer Program Configuration Items (CPCIs) are released for coding, beginning the implementation phase of the contract. After CDR, there are no additional formal technical software reviews until the end of implementation phase when the Functional and Physical Configuration Audits (FCA and PCA) and formal acceptance tests are conducted. Separate fault tolerance risk management activities should be established for:
    - Fault-tolerant infrastructure
    - Error handling in software applications

- **o** Performance monitoring

The fault tolerance mechanisms will generally be developed by individuals whose primary objective is to deliver a working fault detection and recovery capability. Risk management activities associated with the fault tolerance mechanism development are directed toward uncovering logic flaws and timing/performance problems.

In contrast, application developers are *not* primarily concerned with fault tolerance. Their main challenge is to develop the functionality required of the application. Under schedule pressure to demonstrate the required functionality, building in the fault tolerance capabilities that need to be embedded into the application software is often overlooked or indefinitely postponed during the development of the application. Once the development has been largely completed, it can be extremely difficult to incorporate fault tolerance into the applications after the fact. Risk management for software application fault tolerance consists of establishing standards for applications developers and ensuring that the standards are followed.

Risk management of performance is typically focused on the operational functionality of the system. Special emphasis needs to be placed on the performance monitoring risk management activity to make sure that failure detection, failure recovery operations, system initialization/re-initialization, and switchover characteristics are properly modeled.

See Section 7.4 of FAA-HDBK-006A, RMA Handbook for a more detailed discussion of these topics.

Task 5: Design Validation and Reliability Growth

As discussed previously, it is not possible to verify compliance with stringent reliability requirements within practical cost and schedule constraints. There is, however, much that can be done to build confidence in the design and operation of the fault tolerance mechanisms and in the overall stability of the system and its readiness for deployment.

Fault Tolerance Diagnostic Testing – Despite an aggressive risk management program, many performance and stability problems do not materialize until large scale testing begins. The System Analysis Recording (SAR) and the Data Reduction and Analysis (DR&A) capabilities provide an opportunity to leverage the data recorded during system testing to observe the operation of the fault tolerance protocols and diagnose problems and abnormalities experienced during their operation.

For system testing to be effective, the SAR and DR&A capabilities should be available when testing begins. Without these capabilities it is difficult to diagnose and correct internal software problems

Functional Testing – Much of the test time at the FAATC is devoted to verifying compliance with each of the functional requirements. This testing should also include verification of compliance with the functional requirements for the systems operations functions including:

- Monitor and Control (M&C)
- System Analysis and Recording (SAR)
- Data Reduction and Analysis (DR&A)

Reliability Growth Testing – A formal reliability demonstration test in which the system is either accepted or rejected based on the test results is not feasible. The test time required to obtain a statistically valid sample is prohibitive, and the large number of software failures encountered in any major software development program would virtually ensure failure to demonstrate compliance with the requirements. Establishing "pass-fail" criteria for a major system acquisition is not a viable alternative.

Reliability growth testing is an on-going process of testing and correcting failures. Reliability growth was initially developed to discover and correct hardware design defects. Statistical methods were developed to predict the system MTBF at any point in time and to estimate the additional test time required to achieve a given MTBF goal.

Reliability growth testing applied to automation systems is primarily a process of exposing and correcting latent software defects. The hundreds of software defects exposed during system testing, coupled with the stringent reliability requirements for these systems, preclude the use of statistical methods to accurately predict the test time to reach a given MTBF prior to system deployment. There is no statistically valid way to verify compliance with reliability requirements at the FAATC prior to field deployment. There is a simple reason for this: it is not possible to obtain enough operating hours at the FAATC to reduce the number of latent defects to the level needed to meet the reliability requirements.

The inescapable conclusion is that it will be necessary to field systems that fall short of meeting the reliability requirements. The large number of additional operating hours accumulated by multiple system installations will increase the rate that software errors are found and corrected and the growth of the system MTBF.

To be successful, the reliability growth program must address two issues. First, the contractor must be aggressive at promptly correcting software defects. The contractor must be given a powerful incentive to keep the best people on the job through its completion, instead of moving them to work on new opportunities. The first step is to establish initial and final reliability targets from the outset in the System Level Specification. The second step is accomplished during the testing phase by a process called "expunging." The system MTBF is computed by dividing the operating hours by the number of failures. However if the contractor demonstrates that the cause of a failure has been corrected, then the failure is "expunged" from the list of failures. If a failure cannot be repeated within 30 days, it is also expunged from the database.

Thus, if all Program Trouble Reports (PTRs) are fixed immediately, the computed MTBF would be infinite even if the system were continuing to fail on daily basis. This measure is statistically meaningless as a indicator of the system's true MTBF. It is, however, a useful metric for assessing the responsiveness of the contractor in fixing the backlog of accumulated PTRs. Since the Government representatives decide when to expunge failures from the database, they have considerable leverage over the contractor by controlling the value of the MTBF reported to senior program management officials. There may be other or better metrics that could be used to measure the contractor's responsiveness in fixing PTRs. The important thing is that there must be a process in place to measure the success of the contractor's support of reliability growth.

A second issue that must be addressed during the reliability growth program is the acceptability of the system to field personnel. In all probability, the system will be deployed to field sites before it has met the reliability requirements. Government field personnel should be involved in the reliability growth testing at the FAATC and concur in the decision concerning when the system is sufficiently stable to warrant sending it to the field.

See Section 7.5 of FAA-HDBK-006A, RMA Handbook for a more detailed discussion of these topics.

Task 6: RMA Requirements Analysis and Maintenance

NAS-SR-1000 Maintenance – Clearly, if the NAS-SR-1000 is to be effective in guiding the evolution of the NAS Architecture, it has to be a living document. The RMA requirements have been designed so that, with the exception of the Service Threads, they should be largely independent of changes in the NAS Architecture or the NAS-SR-1000 functional requirements. The basic concept of assigning a STLSC to a Service Thread and applying the RMA requirements associated with the STLSC to the Service Thread is independent of the evolution of the NAS architecture.

One of the advantages of the Service Thread based approach is that the Service Threads will remain relatively constant as the NAS Architecture evolves. Many, if not most, of the changes to the NAS Architecture involve replacement of a subsystem represented by a single block in the reliability block diagram for a Service Thread. Thus, the basic thread does not need to change, only the name of a block in the thread. As the NAS evolves, the Service Thread Diagrams should evolve with it.

While the addition of a new Service Thread to the NAS should be a relatively rare occurrence, Service Threads may need to be added in the future to accommodate new NAS capabilities. Provisions should be made so that it is not overly difficult to make these additions. Maintaining a flexible approach to Service Thread mapping will facilitate the accommodation of new threads when they are needed.

RMA Requirements Assessment – The NAS-SR-1000 RMA requirements have been rewritten to allocate RMA requirements to Service Threads that

are based on the National Airspace Performance Reporting System (NAPRS) services defined in FAA Order 6040.15. The Service Thread approach applies the NAS-Level requirements to real-world services and facilities that are precisely defined and well-understood in both the engineering *and* operational communities in the FAA.

Several benefits accrue from using this approach, including the ability to “close the loop” between the measured RMA characteristics of operational services and systems and the NAS-Level requirements for these systems. Previously, the only real feedback reconciling RMA requirements with the actual performance of systems has been part of the WJHTC testing of newly developed systems. Linking the NAS-level requirements to NAPRS operational services allows system engineers to assess the reasonableness of the requirements by comparing them with the achieved reliability and availability of currently deployed systems.

This topic is discussed in more detail in Sections 8 and 9 of FAA-HDBK-006A, RMA Handbook.

RMA Outputs

- **Preliminary Requirements Analysis** – The preliminary RMA requirements analysis has been completed and documented in NAS-SR-1000 and FAA-HDBK-006A.
- **Procurement Package Development** – The following RMA engineering outputs are needed by acquisition managers responsible for preparing the procurement package:
    - RMA- and fault-tolerance-related sections of the System Level Specification
    - RMA- and fault-tolerance-related sections of the Statement of Work (SOW)
    - Data Item Descriptions for RMA- and fault-tolerance-related deliverables
    - RMA and fault tolerance items to be included in the Information for Proposal Preparation (IFPP)
- **Proposal Evaluation**
    - RMA Model Assessment
    - Fault Tolerance Design Evaluation
    - Fault Tolerance Performance Assessment
- **Contractor Design Monitoring**
    - Formal Design Reviews

  - Technical Interchange Meetings
  - Fault Tolerance Design Risk Management
- **Testing and Verification**
  - Fault Tolerance Diagnostic Testing
  - Functional Testing
  - Reliability Growth Testing
- **Requirements Analysis and Maintenance**
  - NAS-SR-1000 Maintenance
  - Requirements Analysis

References

FAA Reliability, Maintainability and Availability (RMA) Handbook, FAA-HDBK-006A, January 7, 2008.

Guide to the Assessment of Reliability of Systems Containing Software. Document No. 89/97714. British Standards Institution, 12 September 1989.

Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Aerospace Recommended Practice, ARP4761. Society of Automotive Engineers, Inc. Issued 1996-12.

Reliability Engineer's Toolkit. Rome Laboratory. Griffiss Air Force Base, April 1993.

System Safety Handbook. Federal Aviation Administration, 30 September 2000.

27 – Life Cycle Engineering

Introduction

Life Cycle Engineering (LCE) is defined as an objective process to evaluate the constraints and dependencies associated with developing and operating a product or service over its entire useful life. Life Cycle Engineering seeks to maximize a product's value while minimizing its cost of ownership over its lifetime. The life cycle includes the entire spectrum of activity for a given system, starting with identification of a need and extending through design and development, production and construction, operational use, sustainment of support and system retirement, and, eventually, disposal.

LCE design considerations address procurement and other issues related to the entire product useful life. It must account for the environment in which the product will operate, as this can affect the product's cost and duration.

Decisions made in early phases of the life cycle affect the overall cost throughout the life cycle. Procurement costs are the most apparent costs associated with the early life cycle. Costs that occur later in the life cycle, such as maintenance costs, are directly related to decisions made in planning and procurement activity. Consequently, LCE focuses on design, implementation, and operational decisions that will significantly impact the product life cycle cost.

Objective

LCE work supports identification of cost/benefit tradeoffs, determines design progress, measures technical soundness, and supports mitigation of risk items. The main objective of LCE is to meet the cost and performance objectives during the entire product life cycle. LCE manages costs from inception (cradle) to disposal (grave) for equipment and projects over their anticipated useful lifespan. LCE aims at providing an engineering discipline that provides best results when both art and science are merged with good judgment.

Life Cycle Engineering Steps

The LCE process consists of six steps—needs identification, technical assessment, technology insertion, operational assessment, performance analysis, and establishment of service environment (see Figure 27-1). Products are produced from executing these LCE steps. Inputs from other System Engineering (SE) elements are required to perform LCE, and LCE products are required to effectively support other SE elements.

LCE activities support the FAA Acquisition Management System (AMS) Life Cycle phases and major decision points. LCE process steps map to these phases. Those same steps identify functional benefits and estimate costs for system features and updates throughout the entire life cycle. LCE uses Earned Value Measurement (EVM) techniques to define cost and schedule targets and provide the metrics for reporting F&E-funded LCE activity status during the Investment Analysis (IA) and Solution Implementation phases.

As IA proceeds for a proposed system procurement, a Basis of Estimate (BOE) document is typically developed to document the underlying cost assumptions and algorithms into a baseline. The estimate must be updated continuously over the program's life to account for cost, schedule, and technical changes and it provides an input to the yearly Resource Planning Document (RPD) submissions. The resulting reports reflect the scope, complexity, and cost performance objectives that the planning activities provide.

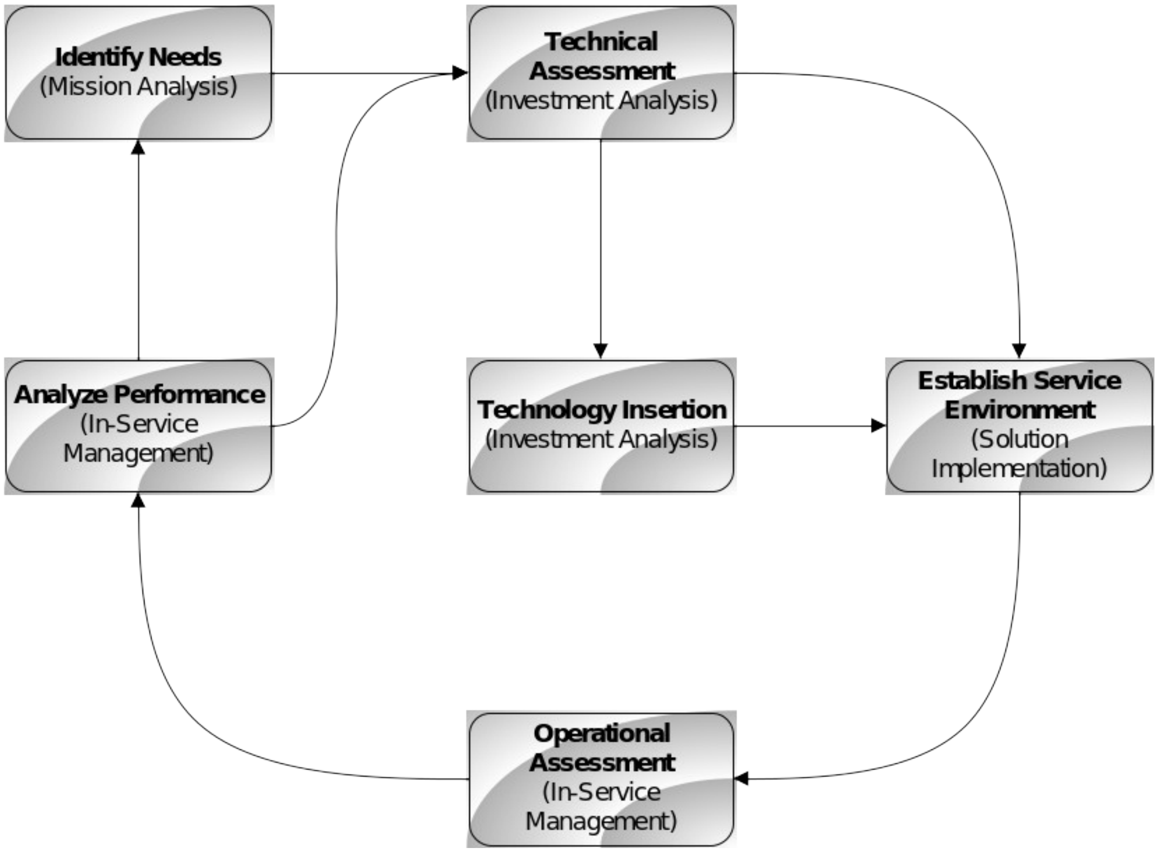


Figure 27-1. LCE Process Steps

The RPD is used not only to describe how and when F&E development dollars are being planned and expended, but also reflects the In-Service Operations funding for system life cycle sustainment.

Step 1: Identify Needs

LCE identifies system life cycle requirements, including real estate management, deployment, and transition; integrated logistics support; sustainment; and disposal. Needs are identified primarily during the Mission Analysis phase of the system life cycle.

Identify LCE Support Needs

LCE depends on defined service levels that detail the support needed from other systems and services in the NAS. These needs, and those of the program, determine the means for delivering projected services. This step identifies the demand for services, as defined in the Service Gap Analysis during the AMS Mission Analysis phase. Often, a system's mission is to extend the capabilities of other services (***e.g.***, system capabilities to meet additional performance requirements). The services being "extended" in this manner are a key element in determining the performance of the system

under question. Changes to the original system will affect the services provided to the system under question, and these changes must be accounted for in the determining the LCE support needs.

For example, the Wide Area Augmentation System is used to augment the integrity of the Department of Defense’s NAVSTAR Global Positioning System to meet the needs of civil aviation.

The system’s program documentation describes the services that support logistical activities and maintenance support capabilities. An example of such a support service definition is the “supply chain” for supplying material to operations. This material is used to deploy new components for sustaining and expanding the system and also for maintaining and repairing in-service components.

Define Logistics Requirements
LCE defines the logistics requirements for supporting the system resources. Typically, resource support is defined in the context of the system’s overall scope and complexity during the entire system life cycle.

Identify Deployment Needs
Deployment of a system into the National Airspace System (NAS) will often be through phases driven by a number of factors, including budget constraints, vendor schedules, technology maturity, service environment, physical infrastructure, and logistics issues. LCE addresses phased deployment and identifies the key events initiating the activities associated with each phase. LCE allocates life cycle costs to each deployment phase, including costs associated with in-service testing, logistics, and maintenance support.

Define Performance Audit Measurements
LCE identifies and specifies operations and maintenance metrics used to evaluate support performance for systems having multiple deployment phases. Support performance requirements are applied to engineering support functions, maintenance personnel, and supply chain components. Technical performance requirements are established as a result of other SE processes (notably Operational Concept (Chapter 11), Functional and Performance Allocation (Chapter 12), Interface Management (Chapter 5), Verification (Chapter 16) and Validation (Chapter 17)).

Develop Logistics Support Metrics
Discrete life cycle activities should be consistent with WBS entries and defined in terms of their entry and exit criteria; schedule and cost criteria are then developed to support these criteria. Avoid level-of-effort approximations, except where existing contracts require it.

Step 2: Technical Assessment

Technical assessment is evaluated at the In-Service Performance Review (ISPR), which is typically held every two years, after commissioning. The ISPR is a formal, technical review to characterize the In-Service technical and operational health of the deployed system by assessing risk, readiness, technical status, and trends in a measurable form that will substantiate In-Service support and budget priorities. (See Technical Assessment (Chapter 9) and Appendix C for additional information.)

This assessment addresses not only potential incorporation of existing technology into design solutions, but also looks at the risks and limits imposed by and on that technology. Each alternative considered is analyzed against the changing technologies available in the marketplace. Available technologies are studied for cost-effectiveness, maturity, for use in the design under consideration, for potential improvements to design performance, and for improvement to maintainability of the resulting system.

The technical assessment may indicate that the system is operating sufficiently (within operational and performance criteria), or it may indicate the need to insert new technology to return the system to operational performance criteria. This assessment also provides input into the Operational Analysis process and ultimately into the mandated OMB-300 reports.

Evaluate Performance Audit

Analyze performance audit results and provide concerns and issues to the Risk Management element.

Evaluate Maintenance Support Facility

Evaluate the Maintenance Support Facility capabilities in supporting system maintenance. The results of this evaluation will include life cycle cost estimates (provided to Requirements Management), and concerns and issues (provided to Risk Management) as work products. This evaluation is especially important as second-level engineering and maintenance support can be over 70% of the program’s operations budget.

Step 3: Technology Insertion

The need for a new technology that makes a previously unavailable performance or functional improvement a viable option must be carefully weighed against the risk imposed by that technology. The potential benefits of inserting the technology must outweigh the potential risks to cost, schedule, and performance. When considering the potential technology insertion, one must consider the impacts to the end user through human factors analysis. (See Chapter 29, Human Factors Engineering)

If the technology assessment indicates new technology is warranted, promising candidate technologies will be evaluated as possible solutions. Some technological opportunities may result, based on the decisions related to the logistics elements. If the decision is to use commercial, off-the-shelf (COTS) products, LCE should identify those items that will probably become obsolete. This creates a need to develop a plan to support all COTS items in the out years of the system's life cycle. The FAA COTS Risk Mitigation Guide/Practical Methods for Effective Acquisition and Support provides information and guidance on COTS product obsolescence stages and how to limit their potential effects on system performance.

LCE recommends preplanned product improvement or alternative improvement options. Inputs may include results of an analysis of the existing system showing opportunities for insertion of technology, the technology assessment, a market survey to identify new products available in the commercial marketplace (COTS), operations and maintenance costs of existing systems, and results of an Investment Analysis.

LCE may conclude that a technological opportunity is beyond the scope of an existing Acquisition Program Baseline. If technology insertion offers a potential for improving safety, significantly lowering costs, or improving effectiveness, then revise the Service Gap Analysis. The updated Needed Capability section should describe the technological opportunity. The description should **not** seek to justify a specific solution or an acquisition program.

Technology Insertion (TI) is also considered the step that defines how systems may replace obsolete components and remain in service. This is a result of system activity that identifies components needing replacement due to lack of support or to achieve technical advantage.

TI includes the following steps:

- Identify technological opportunities during the Mission Analysis Life Cycle phase
- Collect the technical data to support schedule and cost decisions to make the baseline changes
- Define the support equipment to deploy the proposed system changes
- Identify new technology insertion resulting in changes to the maintenance support facility (*e.g.*, second-level engineering support, outsourcing strategies, and other maintenance requirements).

Step 4: Analyze Performance

This LCE step periodically measures the system's performance against the approved baseline (established at the beginning of the LCE steps). The

performance criteria are defined in the design and system performance is evaluated periodically throughout the system's life cycle.

Define Performance Audit Objectives

Performance audits measure the technical performance of a system (or service). They measure each service function provided by the system under consideration for consistency with the service level included with the approved baseline. Since the approved baseline is subject to change over a system's life cycle, a performance audit will verify the service functions for each service level.

Analyze Investment Performance

There are two stages in investment performance analysis. The first is the AMS Initial Investment Analysis phase, which focuses on the set of viable alternatives. LCE provides a life cycle cost estimate for each of these alternatives. An important artifact produced at this time is the preliminary program requirements (pPR). The Final Investment Analysis phase refines the physical architecture for the selected alternative and adds maturity to the documentation. The final program requirements (fPR) and the program specification are completed and finalized. LCE provides a refined life cycle cost based on the fPR.

Steps in the investment performance analysis include the following:

- Identify metrics affected by planned investment objectives. These objectives should support the business by identifying cost, schedule, and technical performance as deviations against the baseline plan.
- Determine life cycle cost based on primary logistical elements, including costs associated with maintaining computer resources support, support equipment (test equipment and tools), and the maintenance support facility over all system life cycle phases.

Step 5: Operational Assessment

At deployment, the system closely matches the baseline fPR. Over time, either the operational needs can change, or the system can deviate from the baseline due to the service environment, either of which requires an operational assessment.

The Service Environment Assessment (OEA) is the key measurement of the operational environment's capability to support the system as it is currently configured, according to the approved baseline. The areas considered in this assessment are also described in the National Airspace Integrated Logistics Support (NAILS) documentation. However, the LCE OEA activity is oriented toward monitoring operational processes and support facilities to achieve the values of the deployed system.

Note: Integrated Logistics Support (ILS) and NAILS are the same and are used interchangeably. FAA documentation refers to both NAILS and ILS. Both are included in this explanation in case one or the other term is used during the course of procurement.

Operational performance is monitored and analyzed, and data is provided as a basis for optimizing current operations and planning for future upgrades. The FAA COTS Risk Mitigation Guide/Practical Methods for Effective Acquisition and Support provides information and guidance on COTS product obsolescence stages and how to limit their potential effects on system sustainment.

LCE, in its data analysis, performs the following functions:

- Monitors and analyzes system performance
- Optimizes current operations
- Identifies technology opportunities and plans for future upgrades
- Identifies obsolescence issues and determines the impact

Step 6: Establish Service Environment

LCE provides the initial scope and complexity assessment for the system or its Service Environment and for any proposed changes. It also manages the system’s life cycle, including real estate management, deployment and transition, integrated logistics support, sustainment, and disposal. It identifies constraints for system life cycle attributes, including:

- Integrated Logistics Support
- Deployment and Transition
- Real Property Management
- Sustainment
- Disposal

Integrated Logistics Support

Integrated Logistics Support, a critical, functional discipline, establishes and maintains a support system for all FAA products and services. The objective is to provide the required level of service to the end user at minimal life cycle cost to the agency. This policy applies not only to new acquisition programs, but also to sustainment of fielded products and services. LCE is responsible for all logistics activities during the life of the system and determines all program logistic attributes.

ILS provides a structured discipline for defining support constraints and acquiring support assets so that fielded products can be operated, supported, and maintained effectively over their entire service life. The primary goal of ILS is to provide high product availability at the lowest cost.

ILS is responsible for identification and acquisition of the support items identified as a result of an analysis of the elements. The nine elements FAA uses that need to be addressed are:

- Maintenance planning
- Maintenance support facility
- Direct-work maintenance staffing
- Supply support
- Support equipment
- Training, training support, and personnel skills
- Technical data
- Packaging, handling, storage, and transportation
- Computer resources support

It is fundamental to sound ILS planning that these elements are addressed within the context of each phase of the product's life cycle (Mission Analysis, Investment Analysis, Solution Implementation, and In-Service Management). It is also necessary to manage the interdependencies among these elements within each phase while adhering to the principles of asset supply chain management (*i.e.*, integration of suppliers, users, and schedules).

ILS determines the parameters of the equipment (reliability, maintainability, and availability). These values will have a direct impact on sparing, depot maintenance, training, maintenance planning, and other elements. The key to a successful acquisition is good communication between the logistics representative and the systems engineer.

ILS Inputs

Several inputs are needed to facilitate effective ILS planning and execution. FAA and Air Traffic Organization (ATO) policy, market research, technology, contractor analysis, and other concerns and issues must be considered.

Additionally, design constraints and trade study reports provide information needed to choose between various alternatives.

ILS Process

The typical steps involved in the ILS process are:

- Develop ILS constraints
- Define maintenance concept and support strategy for candidate solution
- Develop ILS performance, cost, and schedule benefits
- Define strategy for satisfying support requirements
- Define work tasks for obtaining support
- Develop ILS input for the procurement package
- Perform support analysis tasks
- Define maintenance support facility constraints
- Acquire ILS assets

- Conduct In-Service Readiness Review for ILS

ILS Outputs

ILS outputs include the Integrated Logistics Support Planning section of the SEMP or LCP, including maintenance concepts, support requirements, and any related concerns and issues. This planning section describes how FAA will support each logistics element. This plan is developed early in the life cycle, coordinated with systems engineering, and is updated as information is further defined. It forms the basis for the contractor's Integrated Support Plan.

Deployment and Transition

Deployment

Deployment planning prepares for and assesses the readiness of a solution to be implemented into the NAS and is contained in the LCP. Deployment planning is part of a continuous In-Service Review process that begins early in the life cycle management process, usually during development of requirements in the Concept and Requirements Development portion of the AMS Mission Analysis phase. All programs undergo some degree of deployment planning to ensure that key aspects of fielding a new capability are planned and implemented, as well as to ensure that deployment does not create a critical deficiency in other projects.

Transition

Transition involves all work activities for installing the new system at the key site, ensuring all (or most) In-Service Review (ISR) checklist items have been closed, conducting the tests for reaching the In-Service Decision (ISD), and transitioning from the legacy to the new system. It also covers all work activities to install subsequent systems at each operational site and to qualify them for operational service. These activities include the transition planning section of the LCP, which documents how to transition operations and maintenance from the existing system to the new system.

The scope of activities includes preparing the site, installing and testing the equipment, conducting dual operations, familiarizing field personnel with the new equipment, obtaining full operational support, and removing and disposing of replaced assets. Trouble-free deployment and transition requires thorough planning early in the life cycle and cooperation between the service organization, facility team, system contractor, and regional and site personnel during deployment.

Deployment and Transition Inputs

The implementation schedule identifies when each site will receive the new equipment and dispose of the old. The test schedule is used in developing the overall deployment or implementation schedule. FAA/ATO policy will identify the steps for deployment and commissioning.

Deployment and Transition Process

Deployment planning involves coordination among and participation by many critical functional disciplines. Tradeoffs among cost, schedule, performance, and benefits relative to these functional disciplines must also include the impact of deployment and implementation considerations. Deployment planning tools (such as a tailored In-Service Review Checklist) assist in identifying, documenting, and resolving deployment and implementation issues. Methods and techniques include, but are not limited to, a tailored application of generic tools; integration of checklist issues with other emerging issues (such as problem test reports from program tests and evaluation); development of action plans to resolve checklists and other items; and documentation of the results of issue resolution and mitigation.

Consistent deployment planning shall be documented in the contractor's Statement of Work and associated efforts. The results of deployment planning (and issue resolution) activities are briefed periodically (*e.g.*, at acquisition reviews), presented at the ISD meeting, summarized in an ISD memorandum, and audited during the post-ISD follow up and monitoring activities. For more detailed guidance, see chapter 18 (Deployment and Transition).

Deployment and Transition Outputs

Completion of an In-Service Review Checklist and an In-Service Decision allows the system to be deployed to the field, marking the entrance to the Solution Implementation phase of AMS. The final output of deployment and transition is a commissioned system and the disposal of the old system.

Real Property Management

The Real Property Management process ensures recording of all real property assets that FAA owns, leases, and utilizes. Functions of real property accountability— which are to be documented in an automated information system—include, but are not limited to, documentation, verification, and confirmation of the existence of real property records.

The Assistant Administrator for Financial Services records and manages all FAA real property assets. More information is in FAA's Interim Fixed Asset System database.

Real Property Management Inputs

The inputs include a list of space constraints, location of existing equipment, and recommendations for new or modified facilities for the product. Facility drawings showing equipment location, spares storage, support equipment and test benches, and other items that use space will be identified.

Real Property Management Process

The systems engineer performs the following tasks related to property management:

- Determines whether real estate must be acquired for FAA-related projects by identifying space constraints, locations, and the requirement for new or modified facilities
- Notifies real estate experts of the need for purchase and ensures that the property is recorded in the real estate database upon purchase/lease

Real Property Management Outputs

The results of the real property analysis form the basis to determine what real property is required. Real property management uses this recommendation to obtain any necessary property assets (through purchase, lease, or other arrangement) with assistance of real estate experts.

Sustainment

Sustainment is the activity that ensures that the operational system remains at its required capability and quality.

Sustainment Inputs

The Sustainment/Technology Evolution process may need any or all of the following inputs:

- Design constraints
- External pressures
- Operations and maintenance costs
- A list of spares that are difficult or impossible to obtain
- A list of new technology developments and components that can be used to enhance the sustainment of systems
- A list of new commercial products and results from market research
- Demonstrations by vendors

Sustainment Process

The Service-Gap Analysis (SGA) serves as the basis for Investment Analysis and is revalidated at the Investment Decision. LCE shall ensure that logistics inputs are included in this document. As a program proceeds through implementation, fielding, sustainment, upgrade, and eventual replacement, the SGA is revalidated periodically. The service organization, working with the field users, will assess the current performance of existing equipment and provide an analysis of how best to sustain the system, as well as plan for future upgrades or replacements.

The Investment Decision stipulates implementation of any preplanned product improvements. Sustainment resources in the acquisition program baseline are used to upgrade components of fielded products (*e.g.*, printers

or processors) as needed. The objective is to develop evolutionary products and rapidly insert new technology rather than to periodically replace fielded products.

LCE assists the service organization and its systems engineering efforts throughout the life cycle in collecting and assessing data for use in evaluating product or service effectiveness. These activities shall include:

- Tracking and evaluating reliability, maintainability, and availability performance and supportability issues
- Analyzing supportability issues caused by market-driven products and analyzing system or subsystem obsolescence
- Determining the most cost-effective means of avoiding projected supportability shortfalls
- Assessing integration of obsolescence-driven system changes with new constraints
- Evaluating the impact of engineering changes, performance shortfalls, or technological opportunities on ILS products and support services
- Supporting revalidation or development of Preliminary Shortfall Analysis Report

Sustainment Outputs

LCE produces a plan to correct systemic problems, remove defects from systems, and implement planned upgrades. It also produces a list of emerging shortfalls and technology enhancements for future systems. Lessons-learned databases may contain samples of these plans, or the service organization may have examples.

Service Life Extension Programs may be used to keep older systems in the field by incorporating new technology. This may increase the service life of the system and lower maintenance costs.

Disposal

An important element of any product's life cycle is the process used to remove facilities from the operational inventory and ultimately dispose of them. Besides funding concerns, a number of logistics issues shall be considered as a system approaches the end of its commissioned life.

Disposal includes all activities associated with disposal management; dismantlement/demolition/removal; restoration; degaussing/destruction of storage media; and salvage of decommissioned equipment, systems, or sites.

Disposal Inputs

Potential inputs include:

- The implementation schedule for the new system and proposed dates for removal of the existing system

- A list of spares, line replaceable units, documentation, and other items related to the system being replaced
- A list of any hazardous materials or items that need special handling

Disposal Process

SE efforts to support disposal of a system being replaced occur during the new system's implementation phase. The Integrated Technical Planning (ITP) process (Chapter 3) is used to develop a Disposal Plan under FAA Order 4800.2, Utilization and Disposal of Excess and Surplus Personal Property. LCE supports the ITP process in developing a disposal plan that identifies the systems, components, assemblies, and so forth that will be removed, disposed of, or cannibalized; any environmental issues; place of disposition; the person responsible for disposal; and many other factors. Previous disposal plans contain examples of items that should be considered.

LCE shall conduct an assessment of the system to determine the need to scavenge usable parts/subsystems from facilities slated to be decommissioned. This source of usable parts/subsystems is particularly important for items that are no longer being manufactured. This opportunity must be weighed against the costs of component removal, shipping, shop/vendor refurbishment, and warehousing. LCE may require the expertise of an engineering service in determining the existence of any hazardous materials within the system.

Disposal Outputs

Outputs may include:

- A schedule identifying when each existing system will be removed and shipped to a disposal location
- A list of items that contain hazardous materials or precious metals or that need special handling
- A list identifying items that can be used in other systems

Tools

LCE tools include:

Logistics Information System. This is the inventory control and ordering system for the FAA.

Spares Planning Model. This model assists in the provisioning process by estimating the range and quantity of spares based on failure rates, cost, and other factors.

Logistics Management Information guidance. This guidance is used to identify to the contractor the logistics analysis required on the system and the expected outcome.

Bar coding. This methodology is defined in the statement of work. It is used to track spares and configuration management of the system.

FAA Acquisition System Toolset (FAST). This is FAA's reference for all documents and tools used during the acquisition process.

Interim Fixed Asset System database. This FAA database, managed by Financial Services, records real property assets (http://www.faa.gov/aba/html_fm/ifas.html).

References

FAA Acquisition System Toolset (FAST). Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. (http://fast.faa.gov/)

Integrated Logistics Support Process Guide (ILSPG). Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2001. (http://fast.faa.gov/toolsets/ILSPG/)

Jones, James V. *Integrated Logistics Support Handbook*. Second Edition. Special Reprint Edition. New York, NY: McGraw-Hill Professional Book Group, 1998. ISBN: 0070331391.

National Airspace System Maintenance Policy. Order 6000.30C. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 25 January 2001.

Logistics Management Information. MIL-PRF-49506. Washington, DC: U.S. Department of Defense, 11 November 1996.

Utilization and Disposal of Excess and Surplus Personal Property. Order 4800.2C. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 31 May 1996.

FAA COTS Risk Mitigation Guide/Practical Methods for Effective Acquisition and Support, V 3.2 dated 1/2010 (http://fast.faa.gov/syseng/index.htm)

This page intentionally left blank.

28 – Electromagnetic Environmental Effects and Spectrum Management

Introduction

Electromagnetic Environmental Effects (E^3) and Spectrum Management are two closely related areas of Specialty Engineering. Both are involved in handling how various types of radiation affect systems, and how to mitigate such effects. They differ, however, in several ways, and the following sections discuss each area separately, starting with E^3.

Electromagnetic Environmental Effects

E^3 Engineering is the technical discipline dealing with the safe and efficient operation of electronic devices regarding radiated and conducted electromagnetic emissions. This includes both a given system's ability to deal with such emissions from its operational environment and how the device itself affects that environment. E^3 activities seek to minimize how systems are limited by electromagnetic factors, and to document limitations and vulnerabilities that remain after a system's deployment.

Electromagnetic Environmental Effects Engineering

E^3 Engineering is a set of Specialty Engineering analyses/requirements that relate to electronic systems. Such systems range from electric household appliances to integrated circuits.

The Federal Communications Commission (FCC) develops and enforces government regulations related to E^3 and gives special attention to what it calls "digital devices." The FCC defines a digital device as:

> “An unintentional radiator (device or system) that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques;”

These devices must be designed to conform to government regulations on electromagnetic emissions.

Systems Engineering Role

All systems deployed in the NAS must conform to government regulations. E^3 analyses will be performed to ensure that all electronic systems function properly within an operational environment and that they are compatible with nonelectronic elements of that environment.

These analyses will also identify problems that could arise from changes in the environment.

There are many types of E^3 that may affect a system's electromagnetic compatibility. Each type is an individual specialty area. From a broad perspective, the operational requirements are to properly address the electromagnetic environment over the system life cycle. The following sections discuss the individual elements of E^3. (Note: E^3-related definitions appear in American National Standards Institute (ANSI) C63.14.)

The Electromagnetic Environment

The Electromagnetic Environment (EME) consists of the systems and other elements (i.e., humans and nature) that exist within the area where a given system is or may be operated. Identifying and describing the EME is a major part of E^3. This involves describing all electromagnetic interference (EMI) within the environment and vulnerabilities to systems and other elements of the environment.

Systems Engineering Role

The systems engineer must develop a complete description of the normal EME within which the system, subsystem, or equipment may be required to perform. In some instances, commercial, off-the shelf (COTS) systems have defined the *survivable* EME for a system; that is, the most extreme conditions (EMI present) within which the system may operate safely and without degrading its function.

Electromagnetic Compatibility

Electromagnetic Compatibility (EMC) is the ability of a system to function within its EME and not be a source of troublesome EMI. EMC analyses involve evaluating the EME (all EMI present within that environment) and the new system's own EMI emissions.

Two general types of emissions are considered in an EMC analysis that evaluates EMI: conducted emissions and radiated emissions. Conducted emissions are electric currents transferred through physical coupling, such as noise fed back into a device's alternating current (AC) power system. Radiated emissions are EM waves emitted intentionally or unintentionally that may be unintentionally received by other systems. Wires transmit and receive EM signals like traditional antennas. Switching waveforms in circuits generates a wide band of EM emissions.

Systems Engineering Role

The systems engineer uses EMC analysis data to determine if either the new system or the elements of the operational environment

adversely affect each other. EMC considerations are critically important and must be seen as design objectives beyond those required for the basic functional performance of an electronic system. This ensures that a system that functions properly in the laboratory will not have problems when it is deployed within a different EME. FAA-G-2100, paragraph 3.3.2 Electromagnetic Compatibility—a requirement for any acquisition, which references all appropriate FCC rules and FAA-referenced Military Standards—ensures consideration of EMC throughout the system life cycle.

Electromagnetic Susceptibility

EM Susceptibility (EMS) specifically deals with a system's operational failure threshold due to weaknesses or lack of resiliency regarding certain EM conditions. A *susceptibility* is a condition that degrades a system. For example, conducted susceptibility refers to a system's inability to withstand an infusion of noise into its power lines.

A *vulnerable* system is defined as a system with the potential to degrade within certain potential EMEs. Any system may be exposed to different operational EMEs during its lifetime, and vulnerability analysis must be performed to head off potential trouble.

Systems Engineering Role

The systems engineer must ensure that susceptibilities and vulnerabilities are addressed before implementation of a system. For example, devices that run on standard AC power must not be susceptible to sudden brief spikes or losses of power if the power system is affected by lightning or other surges. Similarly, an EMS analysis must be conducted to determine the operational impacts of laboratory-observed susceptibilities and vulnerabilities.

Hazards of Electromagnetic Radiation

Hazards of EM Radiation (RADHAZ) are areas of E^3 that deal with specific types of dangers related to radiated EM waves. The two primary RADHAZ evaluated are Hazards of EM Radiation to Fuels (HERF) and Hazards of EM Radiation to Personnel (HERP). HERF is a RADHAZ area dealing with fuels that may be present within an EME. An EM field of sufficient intensity may create sparks that may ignite volatile combustibles, such as fuel (*i.e.*, EM radiation may induce a current in a conductive material, and form sparks in the air gap between two conductors).

HERP deals with the dangers of EM radiation to humans within the EME. When a person absorbs microwaves, the body heats up. Microwave absorption at high power levels (i.e., from radar towers) is sometimes

hazardous. Also, EM waves in the x-ray range and higher (in terms of frequency) may cause ionization, even at low power levels.

Systems Engineering Role
It is difficult to locate all potential antennas and spark gaps within an EME, so systems engineers need to keep the power densities of EM fields within safety margins when fuels are present. The systems engineer must also consider RADHAZ in the E^3 analysis to ensure safety for the non-electronic elements of an EME, such as humans and nature.

Electromagnetic Pulse
An EM Pulse (EMP) is an intense burst of EMI, such as that caused by a nuclear explosion. This pulse may damage sensitive electronic systems or cause them to temporarily malfunction. Evaluating the need to perform an analysis on EMP susceptibility is recommended.

Electrostatic Discharge
An Electrostatic Discharge (ESD) is an unintentional transfer of static electricity from one object to another. Static voltage transferred from a human to a device (e.g., voltage generated by walking across a carpet) may be as high as 25 kilovolts. The brief currents created may damage or cause malfunction of integrated circuits and other electronics. Evaluating the need to perform an ESD susceptibility analysis is recommended.

Lightning
Lightning gets special attention within E^3 because of its tremendous power levels and multiple effects. Lightning effects are *direct* (physical effects) and *indirect* (induced electrical transients and interaction of the EM fields associated with lightning). Determining a need for analysis for susceptibility to lightning is recommended.

Precipitation Static
Precipitation Static (P-Static) is the buildup of static electricity resulting from an object's exposure to moving air, fluid, or tiny solid particles (e.g., snow or ice). It may cause significant ESD and is a particularly important consideration regarding systems aboard aircraft and spacecraft. Evaluating the need for an analysis on P-Static susceptibility is recommended.

Objective

Beyond their mandatory inclusion through regulations, E^3 activities serve to reduce costs, improve system designs, aid in preventing hazards, and to satisfy international concerns. The benefits and satisfaction of laws make E^3 an indispensible part of any systems engineering endeavor.

Government Regulations

The FCC develops and enforces government regulations relating to E^3. Before a new electronic device may be sold in the United States, it must meet FCC standards. These standards are in Rules and Regulations of Title 47 (Part 15) of the Code of Federal Regulations.

FCC requirements focus on a system's generated EMI, rather than its EMS. The requirements impose limits on the conducted and radiated emissions of digital devices and strictly regulate radiated emissions in terms of the electric field. Most NAS-related electronic/radio frequency devices fall under FCC Class A (commercial, industrial, or business) regulations, which are less stringent than Class B (household devices). Government regulations change frequently, so the systems engineer must ensure he has the current requirements. Information is available from the FCC Web site (www.fcc.gov). The FCC may request a sample device of a new system to test.

System Performance and Cost of Redesign

While manufacturers and developers strive to meet government regulations, they may impose additional E^3 requirements on a new system to enhance product performance and customer satisfaction. Government E^3 requirements do not guarantee a new system's compatibility with its intended operational environment. Thus, it is up to manufacturers and developers to consider the EME for a new system, the impacts of the system's own EMI on that environment, and the system's EMS in order to avoid potential problems that FCC regulations are unable to predict or prevent.

Developers and manufacturers who consider potential E^3 problems from the start may avoid costly redesign later. The earlier in a system's life cycle that a problem is identified, the less the cost of correcting it is likely to be. For instance, if a problem with EMC is discovered after a new system has been deployed, the system may have to undergo extensive redevelopment. However, if this problem had been determined during the design and planning stage, it could have been addressed in the requirements before manufacture had begun, saving both significant time and resources.

Hazard Prevention

Hazards of EM radiation on fuels and personnel (HERF, HERP) are obvious considerations. These issues may be included as part of Safety Risk Management activities, and yet are still considered in E^3.

International Considerations

EMI is increasing throughout the world. Systems that may be used outside of the United States, such as avionics, must be able to deal with types and intensities of EMI present in other countries that may be different from

conditions in the United States. It is recommended that such systems be designed specifically focusing on minimizing vulnerability to EM radiation.

Also, it is recommended that consideration be given to the possibility of intentional jamming, which creates significant EMI.

Analyses of Electromagnetic Environmental Effects

This section specifically discusses the various E^3-related analyses. Not all E^3 analyses discussed are necessary for a given system; which analyses are worth the time and resources are determined during planning.

It is recommended that E^3 analyses be performed on COTS systems as well as new systems to ensure compatibility with the EME within which these systems or subsystems may be used. The amount of detail involved with E^3 analyses increases with each subsequent phase of the SE life cycle. Measurement procedures for evaluating a product's emissions during low-level technical analyses must be clearly spelled out. The EME may undergo appreciable changes at any point during a system's life cycle. Thus, E^3 analyses are redone to ensure continued EMC of *each* system within the EME.

Description of the Operational Electromagnetic Environment

Before any EMC analyses are conducted, the EME within which the new system may perform must be defined. This definition entails detailing all sources of EMI in the operational environment. EME contributors are gauged by the power levels and frequencies of their emissions and their locations (with respect to the new system). In some cases, it may also be necessary to denote inherent susceptibilities associated with other systems within the EME.

An existing OSED document may be useful as a starting point for an EME description. The OSED contains information about the operational environment and the systems/subsystems associated with the new system. However, the OSED may not describe all EME contributors.

Optionally, a description may be developed of the maximum survivable EME conditions in which the system shall be able to function without degradation. This is useful in cases in which a specific, operational EME may not be identified (*e.g.*, the system may have numerous and appreciably different operational EMEs to which it is expected to be exposed).

Electromagnetic Compatibility Analyses

EMC analyses identify compatibility issues relating to radiated and/or conducted emissions. This involves evaluating how the EME and the system affect each other in terms of EMI.

The system's *electrical dimensions* must be calculated before an EMC analysis is conducted. This is done to determine whether or not simple mathematical methods (e.g., Kirchoff's Laws) are sufficiently accurate for an EMC analysis. If the system is *electrically large*, then simple mathematics is insufficient, and Maxwell's Equations shall instead be employed. These are a set of differential equations that describe an electric field as three-dimensional parameters (x, y, z) and time (t).

Federal Communications Commission Regulations

It is convenient to address FCC compliance issues for EM emissions during EMC analyses since both deal with the system's EMI. While actual testing to verify that FCC requirements are met may not occur until a system is built, incorporating these regulations into requirements from the beginning of system development helps to mitigate compliance problems later.

Analyses of Hazards of Electromagnetic Radiation

RADHAZ analyses are conducted only when they have relevance for a particular system and its environment. For example, if there are no fuels present within the operational EME, an HERF analysis is unnecessary. It is recommended that the types of RADHAZ analyses (if any) to be performed be determined from the EME description.

Electromagnetic Susceptibility Analyses

As with RADHAZ, specific susceptibility analyses are conducted only when they have relevance. Each analysis requires time and resources, so it is impractical to invest in an analysis that has no significance for the system and its EME. Susceptibility analyses include:

- Conducted Susceptibility (AC power lines)
- ESD Susceptibility
- Lightning Susceptibility
- P-Static Susceptibility
- EMP Survivability

Outputs and Products of Electromagnetic Environmental Effects

E^3 analyses and predictions must be employed during all phases of an electronic system's life cycle. The following sections link the outputs of E^3 activities to the overall SE process. However, note that all E^3 analyses, like other Specialty Engineering analyses, shall be documented in a Design Analysis Report.

Requirements

Most E^3 activities result in requirements that feed the Requirements Management process (Section 4.3). This includes the Mission Need

Statement, Statement of Work, specifications, and all performance-based requirements.

Concerns and Issues

E^3 activities—in addition to identifying necessary requirements—also identify potential problems that may surface later in a system's life cycle. It is also good practice to document identified system susceptibilities that are not significant enough to require correction. These issues are included with concerns and issues, which feed the Risk Management process (Chapter 6).

Verification Criteria

Verification criteria must be provided to ensure that stated E^3 performance requirements are met. It is also important to provide detailed information describing how E^3 testing is performed and how test results are to be interpreted. This feeds the Verification and Validation processes (Chapters 16 and 17).

Solutions to Problems of Electromagnetic Environmental Effects

EMC and EMS problems may be corrected through a number of means, including shielding, emission suppression components, and/or modification of the operational environment. However, some problems may not be directly correctable, potentially forcing extensive and costly product redesign. This is why it is beneficial to consider E^3 issues early in a system's development.

Spectrum Management

The radio frequency (RF) spectrum is that portion of the EM spectrum used for *intentionally* transmitting and receiving signals. It is a finite set of frequencies that must be divided efficiently between various government and civilian industries. FAA, the Air Force, and the Navy are the top three spectrum users in the Federal Government. FAA's numerous communication, navigation, and surveillance systems heavily depend on the RF spectrum, as evidenced by the agency's more than 50,000 frequency assignments.

Spectrum Management within FAA ensures that systems that use RF technology are assigned proper frequency bands and do not degrade the performance of other RF systems within the NAS.

Definition

FAA Order 6050.19 states that "The radio spectrum, especially aeronautical radio spectrum that is reserved for exclusive worldwide use by international civil aviation, is a scarce and limited resource," and that "The FAA, and civil aviation in general, is committed to the use of new spectrum-efficient technologies and procedures to preserve this precious resource."

Spectrum Management includes distributing FAA's share of the RF spectrum among NAS systems, integrating new RF technologies into the existing NAS, monitoring RF activity to ensure that NAS RF systems do not interfere with one another, and investigating external sources of RF Interference (RFI) that may degrade performance of NAS systems.

Coordination With Technical Operations Services

Technical Operations Services is an FAA line of business within the Air Traffic Organization (ATO) that manages FAA usage of the radio spectrum and resolves RFI issues by maintaining a network of Frequency Management Officers (FMOs). Nationally, FMOs are the aviation community's points of contact for resolving reported cases of RFI. Spectrum engineers assigned to the Regional Frequency Management Offices perform detailed, onsite investigations to quickly resolve RFI cases to keep the NAS operating in an interference-free electromagnetic environment. FMOs can also engineer local or "site-specific" radio frequencies for approval by Technical Operations Services.

The ATO's Office of Technical Operations Services, ATC Spectrum Engineering Services (formerly Spectrum Policy and Management - ASR), oversees Spectrum Management within FAA. All project teams developing systems that require RF usage must coordinate with ATC Spectrum Engineering Services to ensure that all Spectrum Management issues are

addressed correctly, including assigning RF bands. Project teams must contact ATC Spectrum Engineering Services early in the development process and request guidance on spectrum issues.

ATC Spectrum Engineering Services manages FAA usage of the radio spectrum and resolves RFI issues by maintaining a network of Frequency Management Officers (FMOs).

Objective

The safe transport of all individual flights between airports is based on radio frequencies being available and interference free so that all of the aviation systems function properly. FAA's Spectrum Engineering Services Office provides these fundamental services by ensuring radio frequency assets are always clear and available, both now and in the future.

Spectrum Management Is Required for All RF Systems

The National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, is responsible for administering that portion of the spectrum allocated to Federal use. It is empowered to authorize Federal agencies, which demonstrate appropriate needs and satisfy specific requirements, to use the spectrum.

Spectrum Engineering Services (ATC) oversees FAA's assigned RF bands. Project teams developing RF systems must collaborate with Spectrum Engineering Services to obtain specific RF band assignments. Spectrum Engineering Services continues Spectrum Management activities throughout a system's life cycle (e.g., frequency reassignments, RFI investigations).

RF System Performance

Spectrum Management ensures an interference-free environment for RF systems. Without Spectrum Management, RFI would be difficult to control, and the performance of RF systems would be seriously degraded. The limited number of usable existing frequency bands dictates the need to organize, coordinate, and monitor spectrum use.

Activities of Spectrum Management

Spectrum Management activities involve identifying and maintaining an RF system's transmission frequencies.

Initial RF Band Assignments

FAA's Spectrum Engineering Services (ATC) will assign frequency bands for operational use with new NAS systems. A new RF system cannot be introduced into the NAS without obtaining frequency assignments.

RFI Detection and Reporting
New systems must be tested to ensure that they do not transmit noise that may interfere with other RF systems. Spectrum Engineering Services can provide specific testing criteria.

Any external (unaccounted for) RFI that impedes a system's performance during operational use should be reported to the appropriate regional Frequency Management Officer for investigation.

RF Band Modifications
At any point during a system's life cycle, Spectrum Engineering Services may change frequency band assignments for any or all NAS systems. Reassignments may be needed because of integration of new RF systems into the NAS, changes in NAS customer needs, RF spectrum allotment adjustments made by the U.S. Office of Spectrum Management, or international issues. Band assignment modifications can occur on a local, national, or international level. Project teams and systems engineers must be prepared to make frequency band adjustments as required by Technical Operations Services.

Outputs and Products of Electromagnetic Environmental Effects
The following sections link the outputs of Spectrum Management activities to the overall System Engineering process. All Spectrum Management issues shall be addressed directly with Technical Operations Services, ATC Spectrum Engineering Services.

Planning Criteria and Initial Requirements Document
During the early Mission Analysis stage, the RF system team must determine the need for and submit a request for spectrum support to the Spectrum Engineering Services Office. The initial requirements document process is not complete until the Spectrum Planning Subcommittee approves the request. The feedback from Spectrum Engineering Services Office feeds the Integrated Technical Planning process (Chapter 3) and the Requirements Management process (Chapter 4).

Requirements and Constraints
Spectrum Engineering Services may impose requirements and/or constraints on an RF system at any stage of its life cycle. These requirements/constraints feed the Requirements Management process (Chapter 4).

Verification Criteria
Spectrum Engineering Services requires validation for any RF system under development that ensures spectrum usage of the system is within the approved bounds. This feeds the Verification and Validation process (Chapters 16 and 17).

References

For FAA-related subject matter expertise in E^3 and Spectrum Management, contact ATO's Office of Technical Operations Services, Spectrum Engineering Services (ATC). Additional sources of information on E^3 and Spectrum Management include:

Policy Guidelines

NTIA (2011), "Manual of Regulations and Procedures for Federal Radio Frequency Management (May 2011 Revision of the 2008 Edition)," U.S. Department of Commerce, National Telecommunications and Information Administration, Washington, DC.
http://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook

DOT, "Radio Frequency Spectrum Use," DOT Order 5420.3, U.S. Department of Transportation, Washington, DC.

FAA (2000), "Radio Spectrum Planning," FAA Order 6050.19E, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 June 2000.
http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/spec_management/library/view/documents/rfi/RFI_6050_19e.pdf

FAA (2001), "Electronic Equipment, General Requirements," Section 3.3.2 "Electromagnetic Compatibility" FAA-G-2100H, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 9 May 2005
http://www.tc.faa.gov/its/worldpac/standards/faa-g-2100h.pdf

FAA (2002), "Radio Spectrum Plan 2001-2010 (2002 Revision)", U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 September 2002.
http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/spec_management/library/view/documents/RSP_2002.pdf

FAA (2005), "Spectrum Management Regulations and Procedures Manual," FAA Order 6050.32B, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 17 November 2005.
http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/73412

Testing Guidelines

RTCA (1997), "Environmental Conditions and Test Procedures for Airborne Equipment," (With Three Changes Issued), RTCA/DO-160F, RTCA, Inc., Washington, DC. http://www.rtca.org/digest_nm/181-FEB08Frontpage.pdf

DoD, (1999), "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," MIL-STD-461F, U.S. Department of Defense, Washington, DC, 10 Dec 2007.

https://assist.daps.dla.mil/docimages/A/0000/0003/5789/000000607244_000000207288_WAQUATEUOJ.PDF?CFID=39736049&CFTOKEN=90270861&jsessionid=5c30aae09cb9a4345b011a5a2c68214b6b6a

SAE (1999), "Electromagnetic Interference Measurement Antennas; Standard Calibration Method," ARP958, revision D, SAE International, Warrendale, PA, March. http://standards.sae.org/wip/arp958d

IEEE (1977), "IEEE Standard Test Procedures for Antennas," IEEE Std-149-1977, Institute of Electrical and Electronics Engineers, New York, NY. (Reaffirmed in 2003), ISBN 1-5593-7609-0. http://standards.ieee.org/findstds/standard/149-1977.html

IEEE (1998), "American National Standards for Electromagnetic Compatibility - Radiated Emission Measurements in Electromagnetic Interference (EMI) Control-Calibration of Antennas (9 kHz to 40 GHz)," IEEE C63.5-1998, Institute of Electrical and Electronics Engineers, New York, NY. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=741969

Web Sites

www.fcc.gov FCC

standards.ieee.org ANSI/IEEE

www.jsc.mil/jsce3/e3prg.asp Joint Spectrum Center, E3 Engineering Support

This page intentionally left blank.

29 – Human Factors Engineering

Introduction

Human Factors Engineering (HFE) is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: (1) equipment, systems, software, and facilities; (2) procedures, jobs, organizational design, and environments; and (3) training, staffing, and personnel management to produce safe, comfortable, efficient, and effective human performance.

HFE provides the opportunity to: (1) develop or improve all human interfaces with the system; (2) optimize human/product performance during system operation, maintenance, and support; and (3) make economical decisions on personnel resources, skills, training, and costs. HFE activities can be embedded and integrated into the acquisition of systems and equipment in order to lower life cycle costs, improve overall performance, and reduce technical risk. Failure to apply the disciplines of HFE has consistently resulted in development of systems that do not satisfy the needs of the workforce and often results in costly delays and extensive rework.

Objective

The people who operate and maintain the hardware/software are just as important as the hardware and the software themselves. The individuals and teams who operate or maintain the system have different aptitudes, abilities, and training, and they operate the hardware/software under various operating conditions, organizational structures, procedures, equipment configurations, and work scenarios. The total composite of these elements and the human component determines the performance, safety, and efficiency of the system. To produce an effective HFE program for any acquisition, one must not only define the system hardware, software, facility, and services, but also the users (operators and maintainers), their attributes, and the environment in which the acquisition will be used.

Applied early in the life cycle acquisition management process, HFE enhances the probability of increased performance, safety, and productivity; decreases life cycle staffing and training costs; and becomes well integrated into the program’s strategy, planning, cost and schedule baselines, and technical tradeoffs. Changes in operational, maintenance, or design concepts during the later phases of an acquisition are expensive and entail high-risk program adjustments. Identifying life cycle costs and human performance components of system operation and maintenance during

investment analysis and requirements definition decreases program risks and long-term operational costs. These benefits apply to commercial, off-the-shelf (COTS) and non-developmental items (NDI) as well as to developmental programs.

Inputs to the HFE Process

User performance requirements and other inputs to the HFE process come from many sources at various phases of the acquisition, starting in mission analysis. The FAA Human Factors Acquisition Job Aid guidelines are in the FAA Acquisition System Toolset (FAST) and provide basic information regarding integration of HFE activities into the acquisition management process. Product teams must be familiar with human factors concepts and processes to embed HFE principles into their acquisition programs.

The Human Performance Interfaces in Systems Acquisition table, below, identifies and defines many classes of human interfaces that the product team may need to consider as it plans and implements equipment/system acquisition programs. Analysis of these interfaces provides a basis for determining the inputs to the HFE process tasks. These inputs may include new or previously conducted human factors research, studies, and analyses; human factors standards and guidelines; human factors technical methods and techniques; human performance data criteria; or other human-system interaction information.

Table 29-1. Human Performance Interfaces in Systems Acquisition

Human Interface Class	Performance Dimension	Performance Objective
Functional Role Interfaces: For operations and maintenance — role of the human versus automation; functional requirements and tasks; manning levels; and skills and training	Task performance	Ability to perform tasks within time and accuracy constraints under all operational conditions
Information Interfaces: Information media, electronic or hardcopy; information characteristics; and the information itself	Information handling/processing performance	Ability to identify, obtain, integrate, understand, interpret, apply, and disseminate information
Environmental Interfaces: Physical, psychological, and tactical environments	Performance under environmental stress	Ability to perform under adverse environmental stress, including heat and cold, vibration, clothing, illumination, reduced visibility, weather, constrained time, and psychological stress
Operational Interfaces: Procedures, job aids, embedded or organic training, and online help	Sustained performance	Ability to maintain performance over time, during heavy workload, and under emergency and degraded conditions

Table 29-1. Human Performance Interfaces in Systems Acquisition—Continued

Human Interface Class	Performance Dimension	Performance Objective
Organizational Interfaces: Job design, policies, lines of authority, management structure, organizational infrastructure	Job performance	Ability to perform jobs, tasks, and functions within the management and organizational structure
Cooperation Interfaces: Communications, inter-personal relations, and team performance	Team performance	Ability to collectively achieve mission objectives
Cognitive Interfaces: Cognitive aspects of human-computer interfaces (HCI), situational awareness, decision making, information integration, workload and short-term memory	Cognitive performance	Ability to perform cognitive operations such as solving problems, making decisions, integrating information, and maintaining situational awareness
Physical Interfaces: Physical aspects of the system with which the human interacts (*e.g.*, HCI, controls and displays, workstations, and facilities)	Operations and maintenance performance	Ability to attain access and perform operations and maintenance at workstations and worksites, and in facilities using controls, displays, support equipment, tools, job aids, workstation configuration, and other instruments

Addressing the human performance limitations and capabilities would be a daunting task unless the task were divided into its many components and unless human factors were detailed in some descriptive taxonomy of issues. Thus, the potential human factors risks and inputs may be reflected as elements of the human factors areas of interest listed in Table 29-2, below.

Table 29-2. Human Factors Areas of Interest

Human Factors Areas of Interest
1. **Allocation of Functional Roles:** Assigning those roles/requirements/tasks for which the human or equipment performs better while enabling the human to maintain awareness of the operational situation.
2. **Anthropometrics and Biomechanics:** Accommodating the physical attributes of its user population (*e.g.*, from the 1st through 99th percentile levels).
3. **CHI (Computer-Human Interaction):** Employing effective and consistent user dialogues, interfaces, and procedures across system functions.
4. **Communications and Teamwork:** Applying system design considerations to enhance required user communications and teamwork.
5. **Culture:** Addressing the organizational and sociological environment into which any change, including new technologies and procedures, will be introduced.
6. **Displays and Controls:** Designing and arranging displays and controls to be consistent with the operator's and maintainer's tasks and actions.
7. **Documentation:** Preparing user documentation and technical manuals in a suitable format of information presentation, at the appropriate reading level, and with the required degree of technical sophistication and clarity.
8. **Environment:** Accommodating environmental factors (including extremes) to which the system will be subjected and understanding the associated effects on human-system performance.
9. **Functional Design:** Applying human-centered design for usability and compatibility with operational and maintenance concepts.
10. **Human Error:** Examining design and contextual conditions (including supervisory and organizational influences) as causal factors contributing to human error, and considering objectives for error tolerance, error prevention, and error correction/recovery.
11. **Information Presentation:** Enhancing operator and maintainer

	Human Factors Areas of Interest
	performance by using effective and consistent labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields.
12.	**Information Requirements:** Ensuring availability and usability of information needed by the operator and maintainer for a specific task when it is needed, and in a form that is directly usable.

Table 29-2. Human Factors Areas of Interest—Continued

Human Factors Areas of Interest
13. **I/O Devices:** Selecting input and output (I/O) methods and devices that allow operators or maintainers to perform tasks, especially critical tasks, quickly and accurately.
14. **KSAs:** Measuring the knowledge, skills, and abilities (KSAs) required to perform job-related tasks, and determining appropriate selection requirements for users.
15. **Operational Suitability:** Ensuring that the system appropriately supports the user in performing intended functions while maintaining interoperability and consistency with other system elements or support systems.
16. **Procedures:** Designing operation and maintenance procedures for simplicity, consistency, and ease of use.
17. **Safety and Health:** Preventing/reducing operator and maintainer exposure to safety and health hazards.
18. **Situational Awareness:** Enabling operators or maintainers to perceive and understand elements of the current situation, and project them to future operational situations.
19. **Special Skills and Tools:** Minimizing the need for special or unique operator or maintainer skills, abilities, tools, or characteristics.
20. **Staffing:** Accommodating constraints and efficiencies for staffing levels and organizational structures.
21. **Training:** Applying methods to enhance operator or maintainer acquisition of the knowledge and skills needed to interface with the system, and designing that system so that these skills are easily learned and retained.
22. **Visual/Auditory Alerts:** Designing visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response.
23. **Workload:** Assessing the net demands or impacts upon the physical, cognitive, and decision-making resources of an operator or maintainer using objective and subjective performance measures.
24. **Work Space:** Designing adequate work space for personnel and their

Human Factors Areas of Interest
tools or equipment, and providing sufficient space for the movements and actions that personnel perform during operational and maintenance tasks under normal, adverse, and emergency conditions.

HFE Process

The process of integrating HFE into acquisition programs entails numerous technical and management activities. Many of these activities are conducted iteratively through several phases of the acquisition, and often in a nonlinear sequence. Other subordinate activities (e.g., critical task analysis, target audience analysis, cognitive analysis, human-in-the-loop simulation, training needs analysis, and Human-Computer Interface prototyping) are also required. A description of these subordinate tasks is in the FAA Human Factors Acquisition Job Aid or in more detailed HFE reference manuals.

HFE Process Tasks

The following process flow provides an outline and overview of key activities in the HFE process.

Activity 1: Incorporate Human Factors Opportunities and Constraints into the Service Gap Analysis

Using the results from the Mission Analysis, HFE identifies the human performance constraints and issues that need to be addressed or resolved, and provides them to the Strategic and Service Analyses. This information may come from operations and maintenance analyses or concepts and other documents that may offer insights into the effects of HFE performance or cost constraints and limitations on the mission and system. Since most acquisitions are evolutionary, important HFE information may be obtained from predecessor or similar architectures, systems, or subsystem components. Analyses and tradeoff studies may be required to determine the effects of constraints and issues on system performance. The existing literature and lessons learned databases should be reviewed in this case. (See *FAA Human Factors Integration Guide for Mission and Service Area Analysis.* September, 2004.)

Activity 2: Incorporate Human Factors Requirements in Program Requirements

The preliminary, initial, and final program requirements documents contain functional, performance and supportability requirements that do not

prescribe a specific solution. The requirements document defines the essential functional and performance capabilities and characteristics, including those involving the human component. As derived from the results of gap analyses and concepts of operation and maintenance, HFE provides for the requirements document the human performance factors (for example, in terms of task time, error rates, and throughput capabilities) and design compliance factors that impact system design and implementation. Cognitive, physical, and sensory requirements are established for the operator, maintainer, and support personnel that contribute to or constrain total system performance using detailed, vetted scenarios. Any safety hazards, health hazards, or critical errors that reduce job performance or system effectiveness must be defined. Staffing, training concepts, and resource limitations (e.g., staffing limits, allowable training time), including requirements for training devices, embedded training, and training logistics must also be described. (See *FAA Guidelines for Human Factors Requirements Development*, June 2011)

Activity 3: Incorporate Human Factors Assessment in the Investment and Business Case Analysis

HFE provides the full range of human performance and interfaces (*e.g.*, cognitive, organizational, physical, functional, and environmental) to achieve an acceptable level of performance for operating, maintaining, and supporting the system. It provides these to the investment analysis and business case for each alternative being evaluated. The analyses provide information on what is known and unknown about human life cycle costs and risks in meeting minimum system performance requirements. HFE areas relevant to the investment and business case analysis include:

- Human performance (human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, team-versus-individual performance)
- Training (length of training, training effectiveness, retraining, skill maintenance, training devices and facilities, embedded training)
- Staffing (staffing levels, team composition, organizational structure)
- Personnel selection (aptitudes, minimum skill levels, special skills, experience levels)
- Safety and health hazards (hazardous materials or conditions, system or equipment safety design, operational or procedural constraints, biomedical influences, protective equipment, required warnings and alarms)

Activity 4: Incorporate Human Factors Parameters in Program Baselines

The program baselines established at the initial and final investment decisions reflect the solution selected by the acquisition authority for

implementation. Based on this solution, HFE inputs to the acquisition program baselines are those human performance requirements needed to achieve the required level of system performance. These inputs are derived from the specified system performance levels identified in program requirements documents (preliminary, initial, and final program requirements). They reflect a progressive refinement that provides increased definition, greater granularity, and more specificity of relevant human-system performance characteristics. In order to properly incorporate these HFE inputs, the program engineers will need to identify constraints, limitations, and unique or specialized training requirements, staffing levels, or personnel skill requirements.

Also, to the degree possible, the required level of human and system performance must be based on practical measures of operational effectiveness and suitability and be stated in quantifiable terms (time to complete a given task, level of accuracy required, and throughput to be processed per unit time).

Activity 5: Designate Human Factors Coordinator for the Service Organization(s)

The Service Organization designates a Human Factors Coordinator to develop, direct, and monitor HFE activities during system acquisition. This designation needs to occur as early as possible during investment and business case analysis to ensure that human considerations are an integral element of market surveys, tradeoff analyses, and the definition of requirements for candidate solutions to mission need. The Human Factors Coordinator has the following responsibilities:

- Define human impacts and constraints during investment analysis and determine human-system functional, performance, and interface requirements,
- Evaluate human-system interfaces during market surveys, tradeoff analyses, and prototypes,
- Prepare and update HFE portions of program planning documents, procurement packages, evaluation and performance criteria/measures, and data collection efforts,
- Develop and analyze operational scenarios and human-system modeling and simulation for operators and maintainers,
- Review and assess HFE concepts and designs,
- Coordinate HFE efforts and workgroup activities, and
- Coordinate HFE with other system engineering disciplines.

Activity 6: Establish Human Factors Working Group

The Human Factors Coordinator may establish and chair a Human Factors Working Group (HFWG) or some other team to facilitate accomplishment of

HFE tasks and activities. The composition of the HFWG is tailored to the needs of the acquisition program. Membership typically consists of key Service Organization system engineering members and specialists, with outside members participating as needed.

Activity 7: Incorporate Human Factors Strategy and Tasks into the Program Implementation Strategy and Planning

The human factors strategy depends on the size, cost, and complexity of the system to be acquired, as well as the nature and complexity of the human-product interface. It is recommended that the HFE strategy address such factors as:

- Scope and level of HFE,
- HFE roles and responsibilities of organizations and contractors,
- Means for evaluating the human-machine interface and achieving user buy-in,
- Data sources and facilities needed,
- Distribution of funding and other resources,
- Timing and scope of HFE activities, and
- Relationship of HFE with other program elements.

The HFWG may assist in developing strategies appropriate for different types of acquisition programs, such as those that procure non-developmental items, commercial, off-the-shelf products, or fully developed new systems.

The human factors tasks and activities define the HFE work to be done during program implementation. For each task, the program planning documentation assigns the responsible person and organization, identifies any output and the approval authority, specifies when the task is to be completed, and allocates resources. As the program progresses through Solution Implementation (Chapter 23), the human factors portion of the program plan is updated to reflect changes in program strategy or execution and to provide more planning detail as it is developed.

Activity 8: Develop Integrated Human Factors Planning Information

For well managed system acquisition programs, the Service Organization prepares a Human Factors Plan or integrates human factors input to the Systems Engineering Management Plan. This information incorporates input from the various domains of human factors, such as training, staffing, personnel selection, and safety. Recommended content and format are outlined in *FAA Human Factors Acquisition Job Aid, 2003*. Tasks associated with this plan include:

- Defining the operational concept and support concept,
- Describing the target population,

- Defining human/system interfaces,
- Defining human impacts of the system,
- Defining the HFE strategy, and
- Defining HFE implementation tasks, activities, and schedule.

Activity 9: Incorporate Human Factors Requirements into System Statements of Work and Specifications

The System Statement of Work and Specifications translate human-system functional and performance requirements and appropriate HFE work tasks to the contractor in a clear, unambiguous, and contractually binding document. The Statement of Work contains all human factors tasking to be imposed on the contractor, and defines data deliverables in the Contract Data Requirements List (CDRL) and associated human factors Data Item Descriptions (DID). The System Specification addresses the following elements to ensure that required human performance effectively influences system design:

- Staffing constraints,
- Required operator and maintainer skills and skill level,
- Training time and cost for formal, informal, and on-the-job skill development,
- Acceptable levels of human and system task performance when operated and maintained by the target user and maintainer population, and
- Human-system interface requirements.

Activity 10: Include Human Factors in Source Evaluation Criteria

Human performance makes an excellent candidate as an evaluation factor in source selection (Section M of the SOW). By providing vendors a clear indication that the government attributes significant weight to how operators and maintainers perform with the system, the agency sends a strong message that operational suitability and effectiveness are of utmost importance.

Activity 11: Conduct HFE Analyses

The responsible Service Organization oversees, monitors, and reviews HFE analyses conducted by the implementation organization. These analyses may involve:

- Defining and allocating system functions and requirements (human factors requirements analysis, CHI prototyping, staffing analysis, training needs analysis, training effectiveness analysis),
- Analyzing information flow and processing (information requirement analysis, CHI design analysis),

- Estimating operator and maintainer capabilities (task performance analysis, training performance analysis, time and motion study, safety analysis),
- Defining and analyzing physical and cognitive tasks and workloads (task analysis, job design analysis, organizational design analysis), and
- Identifying and measuring human error risks and defining their mitigation and impact on design, equipment, procedures, and task performance (critical task analysis, human reliability analysis for Reliability, Maintainability, and Availability Engineering; human factors safety analysis; and human factors risk assessment).

Activity 12: Apply HFE to System Design

HFE is applied to system design activities to optimize human-system interfaces and to ensure that human performance requirements are satisfied. HFE is applied to the full scope of system design, including experiments, tests, and studies; engineering drawings; work environment, crew station, and facility design; performance and design specifications; procedure development; software development; and job aids, technical manuals and other documentation. The following are used effectively in defining human-product interfaces during system design:

- Prototypes and computer models,
- Three-dimensional mockups,
- Scale models,

- Static and dynamic simulation, and
- Early user evaluation.

Activity 13: Test System Against Human Performance Requirements

To determine if the system complies with human performance requirements, testing is initiated as early as possible in system development. HFE findings from design reviews, prototype reviews, mockup inspections, demonstrations, modeling, simulations, and other early engineering activities/assessments are used in planning and conducting later and more rigorous test and evaluation activities. HFE testing focuses on verifying that user personnel in the intended operational environment are able to operate, maintain, and support the system under normal and off-nominal operating conditions.

Activity 14: Incorporate Human Factors Considerations in Post-Implementation Review

Operational suitability and effectiveness are major evaluation factors that are considered in making the decision to place a new capability into operational service. Satisfactory human performance is an integral element of operational suitability and effectiveness. The broad range of HFE issues is addressed during this activity. Also, a plan is formulated to assess and monitor the human-system performance of the new capability following its deployment to the operational environment, especially for risks and limitations noted during the In-Service Review.

HFE Process Outputs/Products

Efforts to manage the HFE program, establish requirements, conduct system integration, and test and evaluate HFE compliance may result in many major and minor HFE outputs and products. These products include human factors input to the primary acquisition documentation as well as human factors research, studies, and analyses that support program and design decisions and documentation. Examples of these products include human factors risk analyses, human factors benefits analyses, criteria for performance evaluation, prototype designs, and critical task analyses.

The HFE activities and their resultant products are described in more detail in the FAA Human Factors Acquisition Job Aid and other government and commercial HFE manuals, and are reflected in the following five key components of program planning and implementation.

HFE Planning Criteria

HFE planning involves developing detailed concepts of use, user and task analyses, HFE activity schedules, levels of effort, methods to be used, strategy for development and verification, and an approach to implementing and integrating with other program planning. This information is sent to Integrated Technical Planning (see Chapter 2).

HFE Analysis Reports

HFE analysis involves identifying the best allocation of roles/tasks/requirements to personnel, equipment, software, or combinations to meet the acquisition objectives. It includes dissecting functions into specific tasks, analyzing tasks to determine human performance parameters and information requirements, quantifying task parameters to permit evaluation of human-system interfaces in relation to total system operation, and identifying HFE risk areas and safety hazards.

HFE Design and Development Analysis Reports

HFE design and development involves converting mission, system, and task analyses data into: (1) detail designs, and (2) development plans to create human-system information flow and interfaces that operate within human performance capabilities, meet system functional requirements, and accomplish mission objectives as assessed though trade studies. (See Chapter 8)

HFE Test and Evaluation Analysis Reports

HFE test and evaluation involves verifying that systems, equipment, software, and facilities may be operated and maintained within intended user performance capabilities and is compatible with overall system requirements, organizational design, operational tempo, and resource constraints. (See Chapters 15 and 16)

HFE Management and Coordination Analysis Reports

HFE management and coordination involves coordinating with and providing input to reliability, maintainability, and availability engineering; system safety; risk management; facilities and systems engineering; integrated logistic support; and other HFE functions, including biomedical, personnel selection, staffing, and training functions.

References

1. Boff, K., and Lincoln J., eds. *Engineering Data Compendium: Human Perception and Performance. Vols. 1-3.* Wright-Patterson Air Force Base, OH: Harry G. Armstrong Aerospace Medical Research Laboratory, 1988.
2. Booher, H. R., ed. Handbook of Human Systems Integration, New York, NY: John Wiley & Sons, Inc., 2003.
3. Booher, H. R., ed. MANPRINT: An Approach to Systems Integration, New York, NY: Van Nostrand Reinhold, 1990.
4. *Definitions of Human Factors Terms*. MIL-HDBK-1908B, August 1999.
5. Chapanis, Alphonse. Human Factors in Systems Engineering, John Wiley and Sons, Inc., 1996.
6. *FAA Guidelines for Human Factors Requirements Development.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2011.
7. Ahlstrom, V. & Longo, K. *Human Factors Design Standard.* Document HF-STD-001. Atlantic City International Airport, NJ: Federal Aviation Administration William J. Hughes Technical Center, February 2011. (http://hf.tc.faa.gov/hfds/)
8. *FAA Human Factors Acquisition Job Aid*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 2003. http://www.hf.faa.gov/docs/508/docs/jobaid.pdf
9. *FAA Human Factors Assessments in Investment Analysis: Definition and Process Summary for Cost, Risk, and Benefit, v. 1.4b.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2006
10. *FAA Human Factors Policy.* FAA Order 9550.8. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, October 1993.
11. *FAA Human Factors Integration Guide for Mission and Service Area Analysis.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, September 2004.
12. *FAA Requirements for Human Factors Program.* Document HF-STD-004. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2009.
13. Hendrick, Hal W. and Kleiner, Brian M, Macroergonomics: An Introduction to Work System Design, 2001.
14. Meister, D. Behavioral Analysis and Measurement Methods. New York, NY: John Wiley & Sons, Inc., 1985.
15. Wickens, C., Mavor, A., and McGee, J., eds. Flight to the Future: Human Factors in Air Traffic Control. Washington, DC: National Academy Press, 1997.

16. Wickens, C., Mavor, A., Parasuraman, R., and McGee, J., eds. The Future of Air Traffic Control: Human Operators and Automation. Washington, DC: National Academy Press, 1998.
17. Pew, R. and Mavor, A., eds. *Human-System Integration in the System Development Process: A New Look.* The National Academies Press, 2007.
18. Salvendy, G., ed. Handbook of Human Factors and Ergonomics. 3rd edition. Hoboken, NJ: John Wiley & Sons, Inc., 2006.
19. Sanders, M. S., and McCormick, E. J. Human Factors in Engineering and Design. 7th edition. New York, NY: McGraw-Hill, 1993.
20. Wickens, C. and Hollands, J. Engineering Psychology and Human Performance. 3rd edition. Upper Saddle River, NJ: Prentice Hall, 1999.
21. Salas, E., and Maurino, D., eds. Human Factors in Aviation. 2nd Edition. San Diego, CA: Academic Press, 2010.

This page intentionally left blank.

30 – Information Security Engineering

Introduction

Information Security Engineering (ISE) is a specialty engineering discipline within Systems Engineering (SE). The practice of ISE involves the analysis of threats and vulnerabilities to information systems and the assessment and mitigation of risk to the information assets that constitute the system during its life cycle.

Federal legislation, such as the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, and the Federal Information Security Amendments Act (FISAA) of 2012, establishes a clear legal basis for information security risk management of Federal information technology (IT) resources.

Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, establishes policy for managing Federal information resources and implements the law within the Executive Branch. Appendix III of Circular A-130, Security of Federal Automated Information Resources, establishes a minimum set of management controls for Federal programs. Appendix III defines Federal agency responsibilities for the security of automated information and requires that an agency official authorize operation of each IT system.

National Institute of Standards and Technology (NIST), in furtherance of its statutory responsibilities under FISMA, developed publications such as 800-27 (Revision A)*, Engineering Principles for Information Technology Security (A Baseline for Achieving Security);* 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems;* and 800-57, *Guide for Assessing the Security Controls in Federal Information Systems,* that includes best practices for Security Engineering as well as roles and responsibilities.

FAA Order 1370.82A has implemented OMB Appendix III by defining the Security Authorization as the basis for security authorization by the appropriate FAA official.
FAA Order 1370.82A states the FAA basic security policy:

> *The FAA must ensure that security controls are implemented commensurate with the risk and magnitude of the harm that would result from*

> *the loss, misuse, denial of service, unauthorized access, or modification of Federal information assets.*

Further, the order describes roles and responsibilities related to Security Authorization of IT products and systems within the FAA (e.g., Authorizing Official (AO), Information System Security Manager (ISSM), or Certifying Agent (CA)).

The FAA's Acquisition Management System (AMS) provides guidance and a flowchart of the steps to be conducted for ISE under the Security section at http://fast.faa.gov. The FAA procedures and practices for conducting ISE continue to evolve. This ISE section provides system/security engineers and program managers useful references, steps, and processes for effectively integrating Information Security into systems being developed and deployed, emphasizing assessment and mitigation of information security risks and the need to start early in the acquisition life cycle.

Objective

In performing ISE, systems and security engineers apply engineering principles to manage and control system security risk to the operational mission of the enterprise. The ISE process, outlined in the next section, defines the tasks that will produce effective and suitable management, operational, and technical security controls for an FAA system. ISE is conducted during all phases of the system life cycle.

Security risk management, in conjunction with the security policies cited above, produces security requirements, which are statements of the implementation of mitigations to security risks that need to be controlled or reduced. Implementing system design and security controls mitigates security risks to an acceptable level. Successful application of ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of a system's IT assets. IT assets include both data and information.

The SE requirements management element (see Requirements Management chapter) is essential for defining and implementing security controls.

Several factors drive the need to perform ISE and to develop and implement rigorous security controls. Figure 30-1 illustrates these drivers, which are:

- **Information Age Technology and Automation.** The FAA Acquisition Management System (AMS) calls for using or adapting

commercially available IT products to satisfy the agency's mission needs. These commercial, off-the-shelf (COTS) products may contain vulnerabilities that, unless properly identified, controlled, and managed, could cause unacceptable risks to FAA services, capabilities, and functions.

- **Critical Infrastructure and Homeland Security.** Homeland Security Presidential Policy Directive 8 (HS-PPD-8) establishes a national policy for Federal departments and agencies to identify and prioritize critical U.S. infrastructure and key resources and to protect them from terrorist attacks.
- **Aviation Growth—NAS Architecture and Operational Concepts.** The pervasiveness of networked information and the increased interconnectivity of FAA systems significantly broaden the agency's exposure to malicious activities from a variety of sources. Expanded services and capabilities that networking and automation have introduced enable improved performance and efficiency, yet dramatically expand vulnerabilities to systems' confidentiality, integrity, and availability unless FAA properly addresses security.
- **Rising Terrorist and National Threats.** FAA is modernizing its capabilities to ensure that the aviation transportation system is adequately protected from risks to the safety and security of the flying public. Information security supports homeland security, contingency response, and disaster recovery as services and capabilities of the NAS, which is a critical infrastructure for the United States.

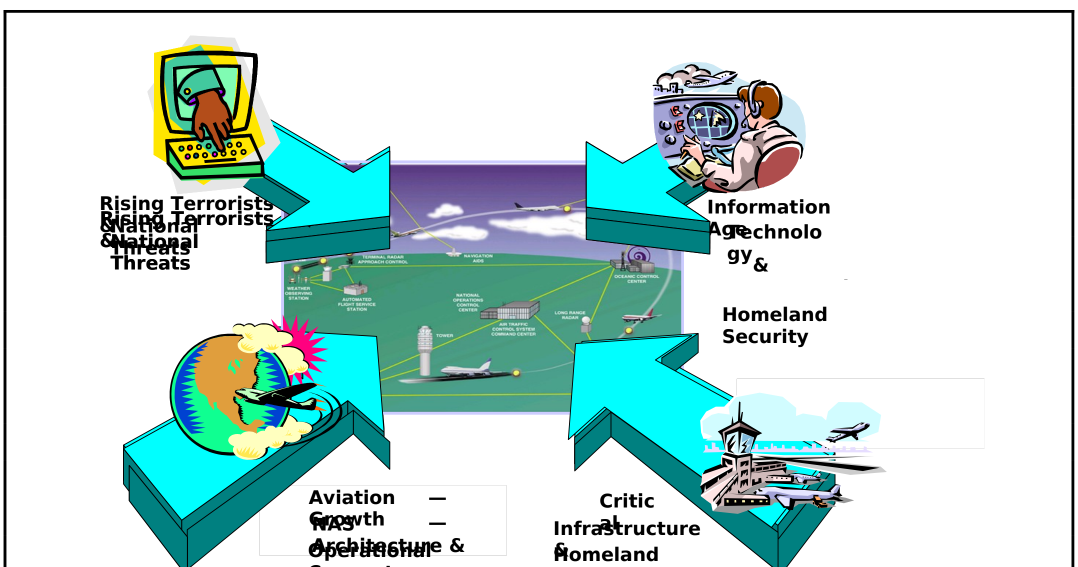


Figure 30-2. Factors Driving Security

These four factors drive FAA toward a more thorough and disciplined implementation of ISE throughout the system life cycle. FAA programs that include security requirements early in development and acquisition typically have lower costs and more effective security features when compared to adding security controls later in the AMS life cycle. The ISE process provides the information security risk management framework within the AMS, from early planning to contract closeout and/or system disposal.

Information Security Engineering Principles

ISE principles provide the foundation for a consistent and structured approach to designing, developing, and implementing information security capabilities that span the system, both logically and physically. Applying ISE principles at appropriate phases of the system life cycle can provide information security, which is a system characteristic. NIST[5] SP 800-27 (Rev. A) identifies 33 ISE principles that should be considered during different phases of the system life cycle. These principles are applicable across the system life cycle, as summarized in Table 30-1, where one check (✓) signifies that the principle can be used to support the life cycle phase, and two checks (✓✓) signify that the principle is key to successful completion of the life cycle phase.

Table 30-1. IT Security Principles (from NIST SP 800-27 (Rev. A)) Versus AMS Life Cycle

IT Security Principles (NIST SP 800-27 Rev. A)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
Security Foundation								
1	Establish a sound security policy as the “foundation” for design.	√√	√√	√	√	√	√	√
2	Treat security as an integral part of the overall system design.	√√	√√	√√	√√	√√	√√	√

[5] The National Institute of Standards and Technology (NIST) is a non-regulatory Federal Agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

IT Security Principles (NIST SP 800-27 Rev. A)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
3	Clearly delineate the physical and logical security boundaries governed by associated security policies.	√√	√√	√√	√√	√	√	
4	Ensure that developers are trained in how to develop secure software.	√√	√√	√√	√√	√		

Risk Based								
5	Reduce risk to an acceptable level.	√√	√√	√√	√√	√√	√√	√√
6	Assume that external systems are insecure.	√√	√√	√√	√√	√√	√√	√
7	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.	√√	√√	√√	√√		√√	
8	Implement tailored system security measures to meet organizational security goals.	√	√	√√	√√	√	√√	√
9	Protect information while being processed, in transit, and in storage.	√	√	√√	√√	√	√√	√
10	Consider custom products to achieve adequate security.	√	√	√√	√√	√	√	
11	Protect against all likely classes of “attacks.”	√	√	√√	√√	√√	√	√
Ease of Use								
12	Where possible, base security on open standards for portability and interoperability.	√	√	√√	√√	√		
13	Use common language in developing security requirements.	√√	√√	√√	√√		√√	
14	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.			√√	√√	√	√√	
15	Strive for operational ease of use.	√	√	√√	√√	√	√√	
Increase Resilience								
16	Implement layered security (Ensure no single point of vulnerability).	√	√	√√	√√	√	√√	√
17	Design and operate an IT system to limit damage and to be resilient in response.	√	√	√√	√√		√√	
18	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.	√	√	√√	√√	√	√√	√
19	Limit or contain vulnerabilities.			√√	√√	√	√	
20	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	√	√	√√	√√	√	√	
21	Use boundary mechanisms to separate computing systems and network infrastructures.			√√	√√	√	√√	

22	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	√	√	√√	√√	√√	√	
23	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.	√	√	√	√	√	√√	
24	Strive for simplicity.	√	√	√√	√√	√	√√	√
25	Minimize the system elements to be trusted.	√	√	√√	√√	√	√√	
26	Implement least privilege.	√	√	√	√	√	√√	
27	Do not implement unnecessary security mechanisms.	√	√	√√	√√	√√	√	
28	Ensure proper security in the shutdown or disposal of a system.			√	√		√	
29	Identify and prevent common errors and vulnerabilities.			√√	√√			
Design with Network in Mind								
30	Implement security through a combination of measures distributed physically and logically.			√√	√√	√	√	√
31	Formulate security measures to address multiple overlapping information domains.	√	√	√√	√√	√	√	
32	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.	√	√	√	√	√	√√	
33	Use unique identities to ensure accountability.	√	√	√	√	√	√√	

The next section illustrates how ISE principles apply to the acquisition process and system life cycle, including establishment of system-level security policy and integration of security into system design, which are two NIST SP 800-27 Rev. A principles.

Reducing information security risk to an acceptable level is a primary ISE principle, and in today's networked world, the concept of risk management is central to ISE. FAA defines information security risk as, "The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack." Mitigating these risks requires solid security risk management, which includes assessment, mitigation, monitoring, and control of security risks throughout the system life cycle.

Based on FAA Order 1370.82A, the appropriate Designated Approving Authority (DAA) determines the acceptable level of risk based on a carefully

considered risk assessment. The DAA determines whether the benefit of operating/connecting the system outweighs the residual risk, which is defined as the combined likelihood of exploits and potential loss or damage to mission capability. The DAA determination considers the operational benefits of the system, the criticality of information, the threats and vulnerabilities, and effectiveness of system features and security controls in addressing security risks.

Integrating system security into the design involves using the following ISE principles (as a minimum) during system development:

- (#8) Address the operational environment of the system and the system's contribution to the FAA mission and services in security policy
- (#3) Delineate clearly the physical and logical boundaries to be governed by the associated system security policies
- (#6) Identify potential tradeoffs between reducing risk and increased costs or impacts to operational effectiveness and suitability
- (#2–#31) Participate during Investment Analysis to identify security concerns and issues, assess system alternatives, and analyze security risks in alternatives. This ensures that the alternatives protect against likely classes of attacks.
- (#28) Include consideration of security features and controls for continuity of operations and disaster response to ensure appropriate availability

Participation in the Investment Analysis phase can improve security requirement statements and avoid costly, specialized controls for security services that may be effectively handled by existing system features, such as management procedures, operational controls, or boundary protection systems/services. Figure 30-2 illustrates the benefit of early ISE involvement in the system life cycle.

Ensures IT protection at affordable cost

Provides disciplined approach to identifying and controlling risks

Builds on FAA practices and procedures for personnel and physical security

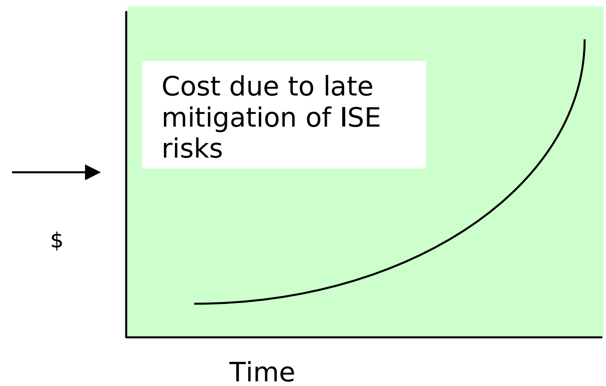


Figure30-3. Benefits of Early Information Security Engineering

Security risk management applies to every AMS phase. The next section integrates guidance from NIST SP 800-30, Risk Management Guide for Information Technology Systems into the FAA Risk Management process model (see Chapter 6). Table 30-2 indicates how risk management activities may be applied during the phases outlined in NIST SP 800-30, as well as the FAA AMS phases.

NIST SP 800-30 Phases	FAA AMS Phases	Support From Risk Management Activities
Phase 1 Initiation	Mission Analysis	Identified risks are used to support development of system requirements, including security requirements, and a security portion of the Concept of Operations (CONOPS).
Phase 2 Development or Acquisition	Investment Analysis	The risks identified during this phase are used to support the security analyses of the system alternatives that may lead to architecture and design tradeoffs during downstream system development.
Phase 3 Implementation	Solution Implementation	The security risk management efforts support assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks requiring mitigation must be made prior to system operation.
Phase 4 In-Service Management	Late stages of Solution Implementation and	Risk management activities are performed for periodic system recertification and reauthorization, or

NIST SP 800-30 Phases	FAA AMS Phases	Support From Risk Management Activities
	In-Service Management, including Technology Refresh	whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces).
Phase 5 Disposal	Service Life Extension	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

Table 30-2. Integration of Information Security Risk Management Into AMS

Information Security Inputs

As Figure 30-3 shows, several SE elements feed ISE. Functional Analysis, Requirements Management, Integrated Technical Planning, Interface Management, and Synthesis feed ISE with inputs, while Integrity of Analysis enables the ISE process. In turn, ISE provides output to other SE elements such as Functional Analysis, Requirements Management, and Risk Management. Note that ISE, like System Safety, conducts risk management separately from—yet it supports—Risk Management.

The ISE process outputs feed other SE processes, becoming integral to SE for the system life cycle. The next section details the ISE outputs and products, while this section discusses the ISE products that result from applying the ISE principles.

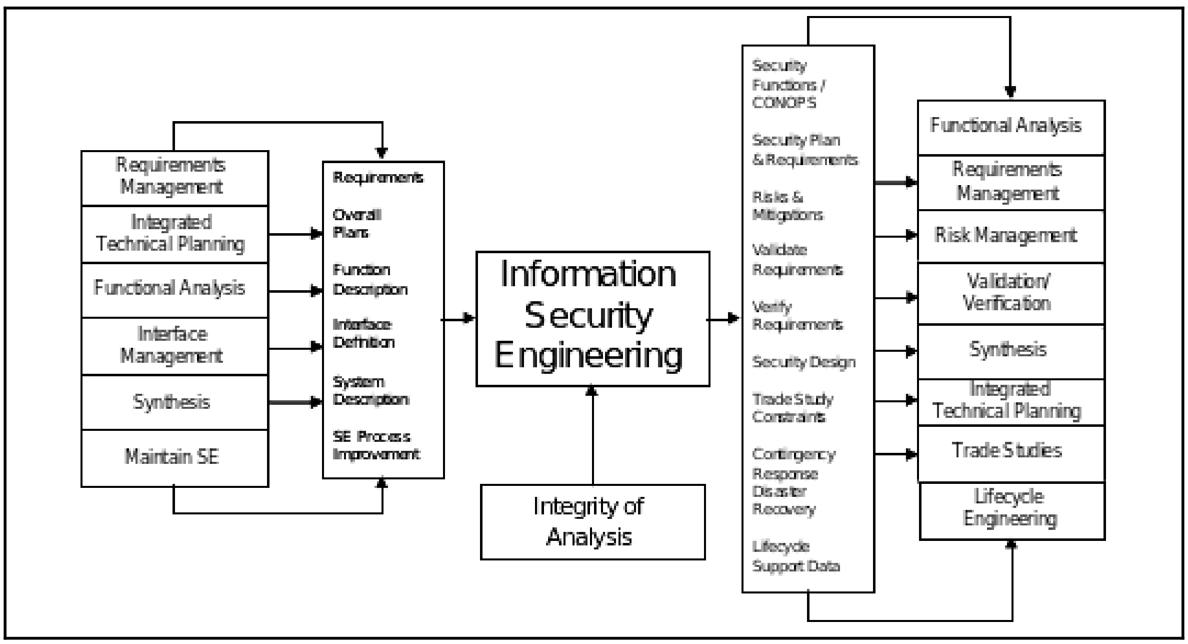


Figure 30-4. ISE Relationship to Other System Engineering Processes

Information Security Engineering Process Tasks

The ISE process tasks support the phased AMS decisions, as shown in Figure Figures 30-4 and -5. Each program or Service Organization shall tailor its ISE activities to meet its program milestones and use its System Engineering Management Plan (SEMP) to tailor its ISE activities and process tasks.

Each phase has ISE products that support the other SE elements, consistent with Figure 30-1, "Specialty Engineering Process-Based Management Chart," and the section on "General Specialty Engineering Process Tasks" (in this chapter). The Information System Security Plan (ISSP) is a key ISE planning document for every FAA IT program. The ISSP provides an overview of the system, presents an approach for meeting associated security requirements, and delineates responsibilities and rules for controlling access and use of information and related assets within the system. The program ISSP is a living document, prepared early in the system life cycle and updated regularly during program/system development. Table 30-3 summarizes the ISE process task alignment with the AMS phases and a more detailed flowchart is found at http://fast.faa.gov.

Legend
ISE Risk Management Process Aligned With AMS
Numbered items correspond to AMS Life Cycle diagram numbers, above

a. Integrate Initial Security Needs and Threat Stipulation into MNS
b. Develop Preliminary ISSP including Basic Security Policy
c. Develop CONOPS and Preliminary Security Requirements
d. Develop Preliminary Vulnerability and Risk Assessment
e. Update Vulnerability and Risk Assessment
f. Update CONOPS and Security Requirements
g. Integrate Security Requirements with System Requirements

Figure 30-5. ISE Process and the AMS Lifecycle Spiral

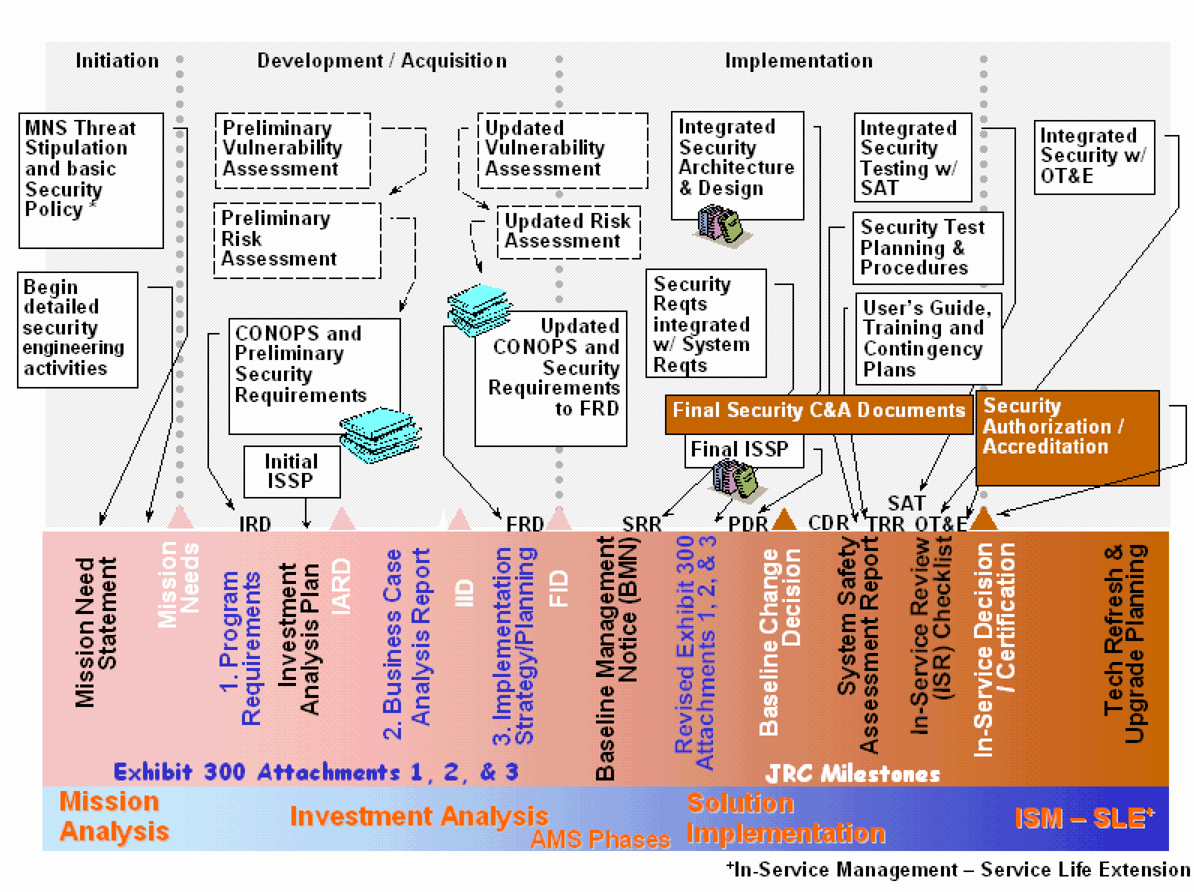


Figure 30-5. Security Activities during the AMS Phases

The following sections summarize the ISE tasks for each AMS phase.

Mission Analysis Phase

The ISE process starts in Mission Analysis. In this phase, the ISE process focuses on the proposed system's operating environment, system boundaries, information assets and functions, and the potential threat and vulnerability sources to the system's information assets and functions. Basic system security policy flows from FAA organizational directives, such as FAA Order 1370.82A, as well as from FAA operating procedures and instructions. Basic system security policy is the set of rules governing control, access, and use of system information. For example, a basic security policy statement may be that only authorized FAA users shall access the system. The ISE process applies Federal Information Processing Standards (FIPS) 199-1 to categorize system information assets and functions. The ISE process analyzes the system and NAS concept of operations (CONOPS) and mission need statement to formulate a basic security policy. The security planning

aspects of ISE also begins in this phase, following guidance of NIST SP 800-18. Security requirements, based on security policy, are in the preliminary Program requirements document.

Investment Analysis Phase

Integrating the ISE process with SE elements is essential. During initial investment analysis, ISE develops and documents the security CONOPS and the initial security requirements for the initial Requirements Document. The investment analysis team uses the CONOPS and security requirements to evaluate system alternatives. Security engineers on the team conduct a preliminary risk assessment using updated threat and vulnerability data to determine specific risks that must be controlled/mitigated. Security trade studies are performed to evaluate system alternatives and to assess security risk controls/mitigation measures related to the system alternatives. Also, security trade studies identify native, existing system, and/or network features that reduce the likelihood of system threats successfully exploiting a vulnerability. These trade studies compare costs and benefits of system features/security controls in terms of risk reduction. Trade studies may evaluate the cost-effectiveness of different controls for a given risk or set of risks. Also, system alternatives may require different types of controls to balance system performance and security requirements against the security risks/costs of different alternatives. Different system alternatives may have significantly different physical and/or system architectures that would require different security controls, which lead to different security costs and effectiveness.

During the final stage of the Investment Analysis phase, ISE refines and updates the preliminary risk assessment. Updated threat and vulnerability data is applied, analyzing the costs and effectiveness of system features and security controls that are associated with each of the final system alternatives. ISE provides final security requirements for the final Program Requirements Document and the system specification, as well as special requirements for the Solicitation Information Request (SIR) and contract Statement of Work (SOW). In developing the final system requirements, ISE analyzes and establishes the appropriate assurance level to be proven during system implementation. Assurance in this context addresses the required level of confidence in the security function and performance and ensures that the security controls function in an integrated fashion. Assurance can be gained through many techniques, including conformance testing, independent verification testing, and employing diverse and/or redundant capability.

ISE shall support a documented agreement among FAA stakeholders regarding the necessity and sufficiency of the security requirements. Clearly documenting the agreement to security requirements before the Investment Decision becomes the foundation for the Security Certification and Authorization Package, which shall be completed before the In-Service Decision. During the investment analysis, ISE identifies the technically qualified, senior FAA official who shall certify that the system security controls meet the minimum FAA/NAS ISS requirements (see DAA discussion, above). The ISSP, which was based on NIST SP 800-18 and was a conceptual draft during the Mission Need phase, is updated to become an initial draft.

The ISE products from this phase include the updated preliminary risk assessment, final security requirements, security trade studies to support cost-benefit/investment analysis of security controls, and input to the SIR, SOW, system specification, and Contract Data Requirements List (CDRL) for systems to be acquired. These products support the AMS milestone decision for transition into the Solution Implementation phase.

Solution Implementation Phase

The ISE activities during earlier phases provide the basis for updating, monitoring, and controlling system security risks and the respective mitigation measures or controls that are implemented during this phase of system development. A summary of ISE activities for this phase includes the following:

- Revise the security CONOPS and security requirements based on functional analysis performed during early stages of the Solution Implementation phase.
- Analyze the physical/system architecture, resulting in an allocation of the security features to be implemented in the system under development. Security trade studies may be needed to identify the appropriate security controls to be implemented that balance system and security requirements.
- Integrate the security features into the security architecture to balance them with the system architecture and design. Security trade studies, interface security requirements, and other SE outputs contribute to successful integration of security architecture into system design. System design reviews are key milestones for ensuring that security controls are integrated into system development.
- Update the ISSP based on the expected ISS functional and assurance controls derived from the system architecture and design. Refine system test planning and procedures to ensure that all security requirements and controls are addressed. The ISSP supports Validation (Chapter 17) and Synthesis to assess controls and assurance

as being cost effective and meeting the ISS requirements. Use Risk Management (Chapter 6) and Requirements Management (Chapter 4) to mitigate security risk to acceptable levels. The criticality/sensitivity of the system and its information assets guides the type and level of controls and testing.

- Develop a users' guide, training plans, and contingency/disaster recovery plans. Security procedures, rules, training, and planning for contingency and disaster recovery operations may be integrated into the integrated logistics support and life cycle planning for systems.
- Conduct security testing. Security controls and mechanisms may be tested incrementally and as a part of system development testing. For mission-critical systems, a third party shall conduct independent testing of system vulnerabilities.
- Create final security Certification and Authorization (C&A) documents. The results of ISE activities—including relevant results from related SE elements such as Integrated Technical Planning (Chapter 3), Validation and Verification (Chapters 17 and 16), and Life Cycle Engineering (Chapter 27)—shall be considered as final security C&A documents. The Air Traffic Organization provides templates for collecting and presenting C&A documentation.

In-Service Management Phase

Activities during this phase include the following:

- Obtain security C&A. Stakeholder C&A review shall ensure that the Designated Approving Authority is in a position to certify and authorize the system as meeting security requirements and as presenting an acceptable risk to the FAA mission and NAS operations.
- Conduct performance measurement, monitoring, and reporting of security controls and incidents. Ensure that monitoring of ISS performance and assurance for the respective NAS service/capability has not degraded and that new vulnerabilities have not been introduced to the operational system.
- Update the C&A package to reflect any major configuration changes at least every three years, assessing changes in the environment and system for previously unforeseen risks from new threats and vulnerabilities. Plan and take corrective action as necessary.
- For disposal of the system, the following types of activities may be addressed in the Information System Security Plan, and conducted at the appropriate stage of the System Development Life Cycle
    - Archive Information—retain information as necessary, keeping in mind legal requirements and future technology changes that render the retrieval method obsolete.

- o Sanitize Media—ensure data is deleted, erased, or written over as necessary.
- o Dispose of Hardware and Software—dispose of the hardware and software in accordance with ISS policy.

Table 30-3 relates the required C&A package to the ISE process steps that provide the conceptual, initial, draft, update, and final results for the C&A package.

Table 30-3. Authorization Documents Related to Information Security Engineering Process

Authorization Documentation	ISE Process Source	How To Reference
System Characterization	ISE h, Draft ISE i, Draft	Security Risk Assessment Methodology and System Characterization Template
Information System Security Plan	ISE b, Conceptual ISE d, Draft ISE i, Update ISE m, Final	Security Risk Assessment Methodology and ISSP Template
Risk Assessment Report (Includes Threat and Vulnerability Assessments)	ISE d, Initial ISE e, Update ISE m, Final	Security Risk Assessment Methodology and Risk Assessment Report Template
Security Test Plan and Test Results Report	ISE e, Initial ISE g, Draft ISE j, Update ISE m, Final	Security Risk Assessment Methodology and Security Test Plan and Test Results Template
Risk Mitigation/Remediation Plan	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Risk Mitigation/Remediation Plan Template
Contingency/Disaster Recovery Plan	ISE i, Initial ISE k, Draft ISE m, Final	Security Risk Assessment Methodology and Contingency/Disaster Recovery Plan Template
Executive Summary	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Executive Summary Template
Authorization Certificate	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and C&A Statement Template

Information Security Engineering Outputs/Products

The important aspect of security outputs/products is to embed security into the program products where possible to minimize treating security as a “standalone” component. The ISE process generates the following output and products.

Information System Security Plan (ISSP)

The system owner (Information Systems Security Certifier) or Service Level Mission Need (SLMN) sponsor shall initiate the ISSP during mission needs analysis. The ISSP evolves during the system’s life cycle, driven by the progression of system development. The ISSP is updated and revised based on ISE activities or other SE activities. To further guide planning, Table 30-4 relates the ISE activities and products to both the AMS milestone products and SE products. Analysis products outlined in the section below are used to update the ISSP.

Table 30-4. Acquisition Management, System Engineering, and Information Security Engineering Relationship

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 30-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Initial requirements, Initial functional architecture, Threat analysis criteria, OSA	Integrate Initial Security Needs and Threat Stipulation into the SLMN	Statement of security policy and threat environment stipulation	New/updated SLMN Draft pPR, including the concept of use; Initial investment analysis plan System Investment Analysis Review
			Requirements Management, Functional Analysis, Synthesis
CONOPS, Initial requirements, analysis criteria, OSA	Develop CONOPS and Preliminary Security Requirements	Initial Security requirements, CONOPS	Business case analysis report Updated pPR for each alternative under serious consideration Initial investment analysis plan Acquisition strategy in the ISAP for each alternative under serious consideration
			Requirements Management, Functional Analysis, Conceptual functional architecture, Synthesis, ITP
FAA Policy, Standards, NAS Architecture, OSED, CONOPS	Develop Preliminary ISSP (Including Basic Security Policy)	Preliminary ISSP with security policy statement	Final SLMN CONOPS Final Investment Analysis Plan Initial description of alternatives
			Requirements Management, Functional Analysis, RVCD, Trade Studies, Interface Management, SEMP
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	Develop Preliminary Vulnerability and Risk Assessment	Preliminary Vulnerability and Risk Assessment	fPR Final investment analysis report Final Exhibit 300 Final ISAP
			Requirements Management, RVCD, VRTM, OSED, Specialty Engineering, Risk Management, Validation, SEMP
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control	Update the Vulnerability and Risk Assessment	Updated Vulnerability and Risk Assessment	SIR System Specification SOW CDRL Source selection criteria and plan

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 30-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Documents, Initial VRTM, Stakeholder Needs			Requirements Management, Specialty Engineering, Risk Management, Validation
CONOPS, Initial requirements, analysis criteria, OSA	Update the CONOPS and Security Requirements	Updated Security requirements, Updated CONOPS	Requirements Management, Functional Analysis, Trade Studies, Interface Management, Configuration Management
CONOPS, Final Security requirements, Security concept of use	Integrate Security Requirements with System Requirements	Initial Verification Requirements Traceability Matrix, Interface Requirements Documents	System Requirements Review System Design Review – PDR
			Requirements Management, Integrated Technical Planning, Trade Studies, Synthesis, Interface Management, Configuration Management, Risk Management
Physical Architecture, Final Security Requirements, Design Analysis Report, Functional Architecture	Integrate Security Architecture and Design	Updated Physical Architecture, Functional Architecture	System Design Review — CDR System Capability Demonstration
			ITP, Requirements Management, Functional Analysis, Synthesis, Interface Management, Risk Management, Configuration Management
Physical Architecture, Functional Architecture, Risk Mitigation Plan, Updated Baselines, Updated CONOPS, FAA Policy, Interface Control Documents, Program Risk Summary	Update the ISSP	Updated Information System Security Plan	ISAP Integrated Life Cycle Plan System Test Plan OT&E Plan
			ITP, Specialty Engineering, Configuration Management, Life Cycle Engineering
Verification Requirements, Traceability Matrix, Risk Mitigation			System Test Plan OT&E Plan

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 30-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Plans, Interface Control Documents, Test and Assessment Articles, Physical Architecture, Functional Architecture, Functional Specification, Master Verification Plan	Develop Security Test Plans and Procedures	Security Test Plan, Security Test Procedures	Integrated Technical Planning, Requirements Management, Interface Management, Verification, RVCD, VRTM
Trade Study Reports, Operational Services and Environmental Description, Functional Specification, Government and International Regulations and Statutes, FAA Policy, Requirements	Develop User's Guides, Training, and Contingency Plans	Contingency and Disaster Recovery Plan, User's Guides, Security Awareness Training (see 4.14)	Integrated Life Cycle Plan Functional Configuration Audit Physical Configuration Audit
			Functional Analysis, Configuration Management, Trade Studies, Specialty Engineering, Verification, ITP
Updated Verification Requirements Traceability Matrix, Requirements Verification Compliance Document, Verification Criteria, Updated Master Verification Plan	Conduct Security Testing	Updated Risk Mitigation Plan, Security Test Report	Test Readiness Review Qualification Test Final Acceptance Test Site Acceptance Test
			Verification, Integrated Technical Planning, Requirements Management, Configuration Management, Risk Management
Risk Mitigation Plan, Program Risk Summary, Updated ISSP, Contingency Plans, Test Validation Reports,	Create Final Security C&A Documents	Certification Package	In-Service Review Checklist OT&E Report
			Specialty Engineering, Configuration Management, Synthesis, Risk Management
Certification Package, FAA Management Decisions, Government and International Regulations and Statutes	Obtain Security Authorization/ Accreditation	Finalized Certification Package	Specialty Engineering, Configuration Management, Synthesis, Risk Management

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 30-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Validated Need, Stakeholder Needs, Integrated Life Cycle Plan, Updated Acquisition Program Baseline, External Environmental Forces	Prepare for Tech Refresh and Upgrade Planning	Updated Security Requirements, Updated Security Certification Package, Updated Vulnerability and Risk Assessment	Life Cycle Engineering, Trade Studies, Configuration Management, Risk Management, Functional Analysis

Analysis Products

The risk assessment methodology described in this section guides collection of security analysis results and recommendations into products that support security accreditation of the service/domain/system. This methodology illustrates how ISE work products are used to validate and verify the security requirements of a given system. The work products are generated according to the individual ISSP for each FAA service/domain/system. Figure 30-6 indicates the type of closed-loop security risk management that is applied during the AMS phases consistent with FAA ISS Policy Order 1370.82A.

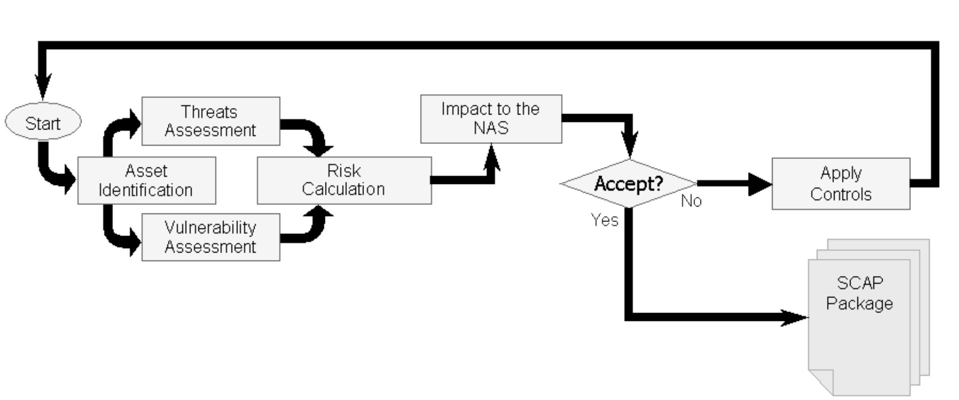


Figure 30-6. Closed-Loop Security Risk Management

This closed-loop method of risk management supports the FAA risk management process model described in Risk Management (Chapter 6), as shown in Figure 30-7, below.

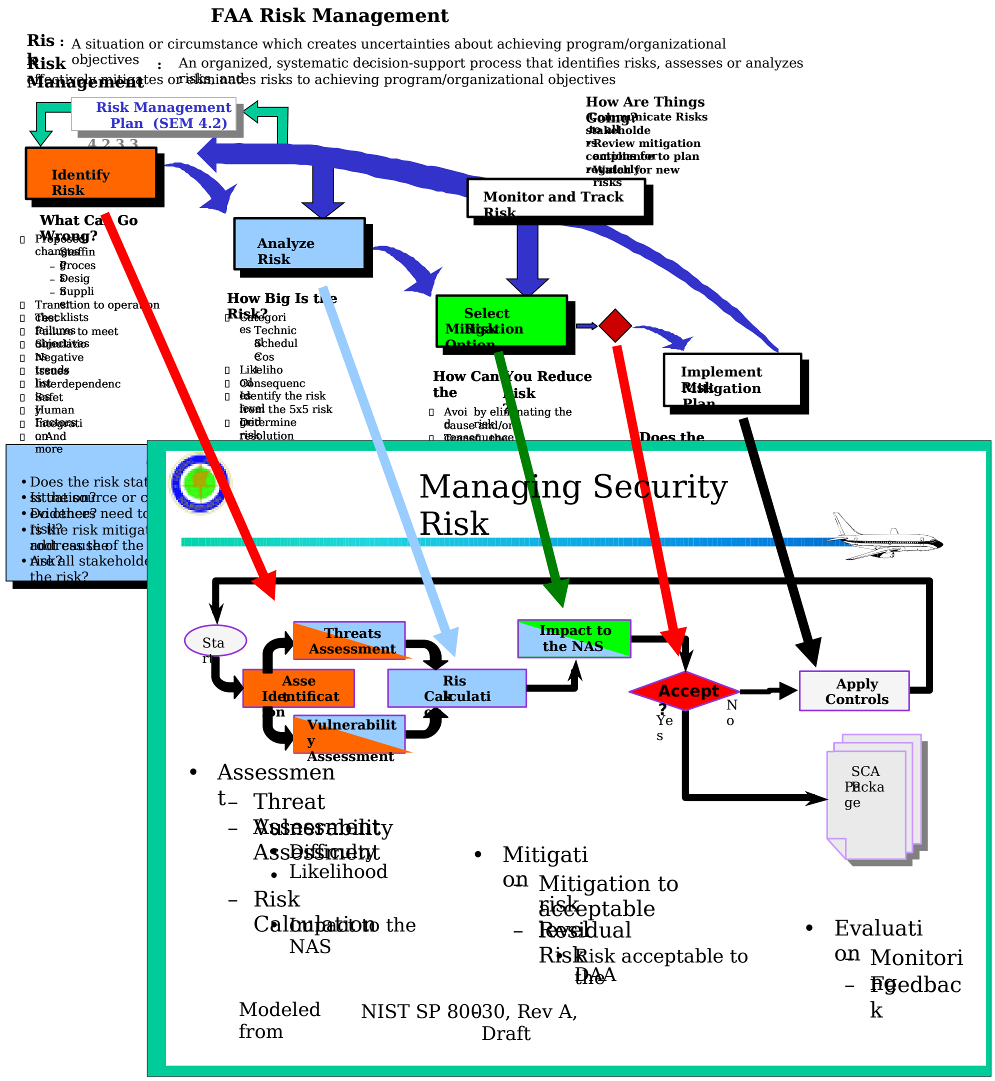


Figure 30-7. Correlation of Information Security Methodology With FAA Risk Management Model

The ISE Risk Assessment Matrix (Figure 30-8) can be used to analyze individual security risks. The matrix reflects the level of risk associated with the **likelihood** of a given threat source exploiting a given vulnerability and the **impact** of that threat source successfully exploiting the vulnerability. Risks to IT systems arise from events such as, but not limited to, the following:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or man-made disasters

- Failure to exercise due care and diligence in the implementation and operation of the IT system

To use the matrix, apply the determined **likelihood** value generated for each threat-vulnerability pair and apply the **impact** rating, considering the vulnerability is successfully exploited. Locate the **likelihood** value in the vertical column and the **impact** rating in the horizontal column. The **Risk Level** is where the two values intersect.

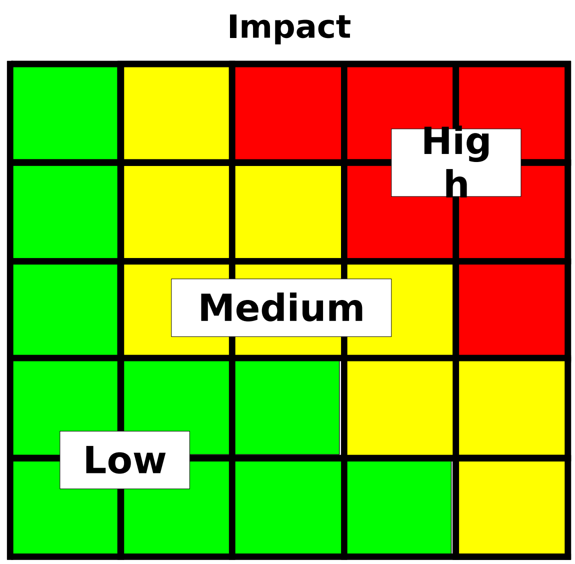


Figure 30-8. ISE Risk Assessment Matrix

Information Security Engineering Tools

There is not a specific set of tools for use in implementing Information Security. Tools should be chosen based on the desired final products and interoperability with other tools used in other SE elements. Tools can be used for discovering vulnerabilities, performing risk assessments, and for tracking and reporting the status of security controls.

Information Security Engineering Metrics

Security requirements should be implemented as early in a program as possible to avoid reworking the program after security requirements are introduced. This can be measured by reviewing the program to see if it meets these standards and that the requirements are implemented. This can be accomplished by ensuring security requirements are included in the plans of action and milestones (POA&M). Guidance for developing these metrics is in NIST Special Publication 800-55, *Performance Measurement Guide for Information Security*.

References

1. Clinger-Cohen Act of 1996.
2. FAA Order 1370.82, *Information Systems Security Program.*
3. Federal Information Security Management Act (FISMA) of 2002.
4. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems.*
5. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems.*
6. *OMB Circular A-130, Management of Federal Information Resources.*
7. *OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.*
8. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*
9. NIST Special Publication 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).*
10. NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.
11. NIST Special Publication 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems.*
12. NIST Special Publication 800-55, *Performance Measurement Guide for Information Security.*
13. NIST Special Publication 800-57, *Guide for Assessing the Security Controls in Federal Information Systems.*

This page intentionally left blank.

31 – System Safety Engineering

Introduction

System Safety Engineering (SSE) is a Specialty Engineering discipline within systems engineering (SE). It is required that system/safety engineers and program managers refer to FAA's Safety Management System (SMS) Manual and the Safety Risk Management Guidance for System Acquisition (SRMGSA) for detailed information about planning and conducting SSE. The following paragraphs describe how system safety is integrated into a system's overall SE.

Definition

SSE is the application of engineering and management tools—including principles, criteria, and techniques—to optimize the safety of a system within the program's operational and programmatic constraints. These tools are used to identify, evaluate, and control hazards associated with a system. A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment. SSE's goal is to identify proactively the hazards in a system early, to continuously assess the risk (severity and likelihood) of each hazard, and to actively control the highest risk hazards. The SRMGSA (available on FAA's FAST Web site) provides more information on this topic.

As illustrated in Figure 31-1, the SSE process is a closed-loop method of Safety Risk Management.

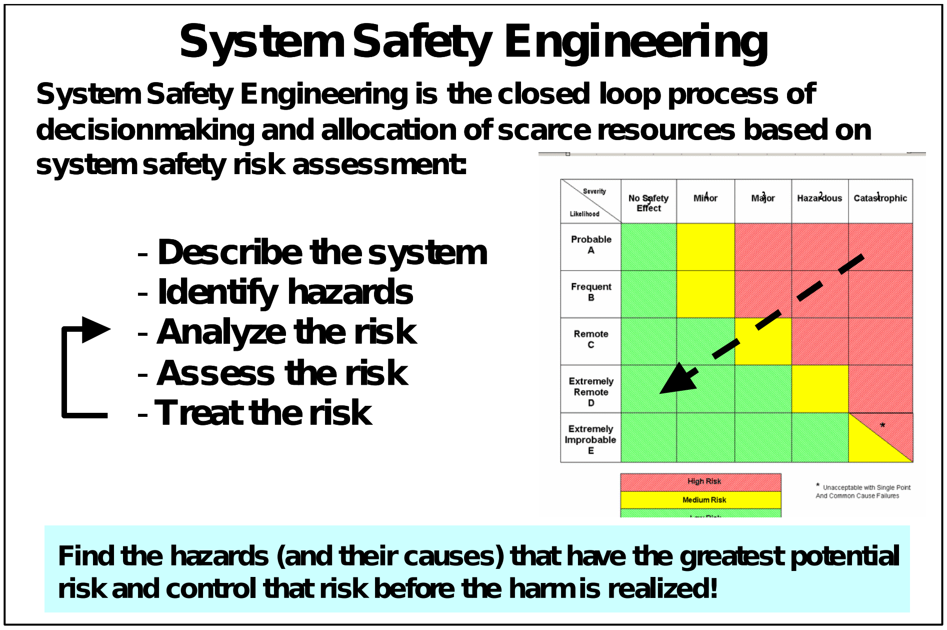


Figure 31-1. Closed-Loop Method of System Safety Engineering

The following documents describe how SSE is conducted in the AMS:

- FAA's SMS Manual
- SRMGSA

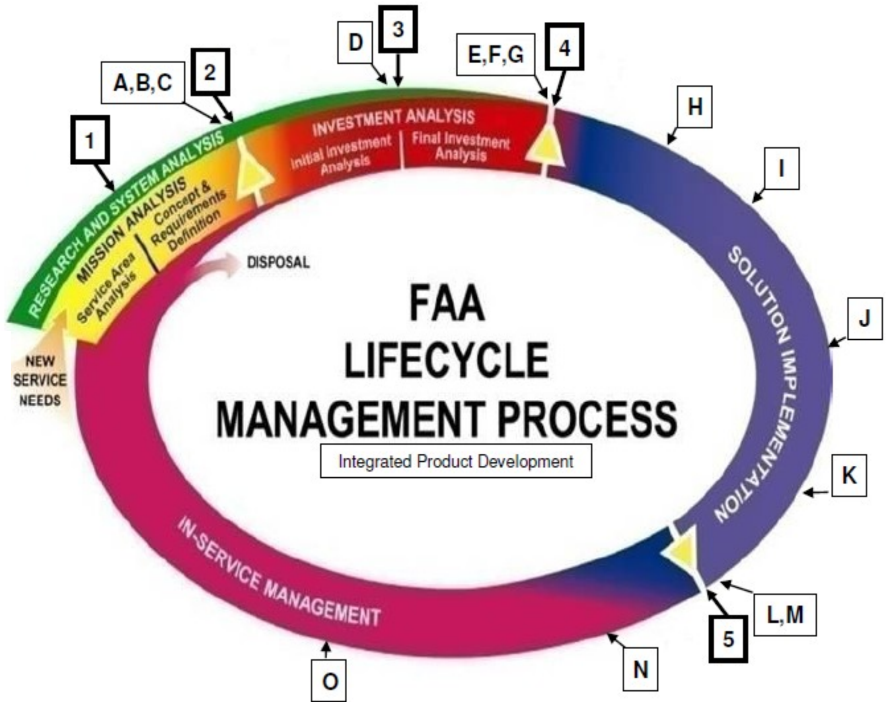
Figure 31-2 shows what safety analyses are performed, relative to the phases of the AMS. These analyses are timed to best support the phased needs and decisions in the overall AMS process.

DECISION POINT LEGEND

1 Concept & Requirements Definition Readiness Decision
2 Investment Analysis Readiness Decision
3 Initial Investment Decision
4 Final Investment Decision
5 In-Service Decision

PRODUCT LEGEND

A Operational Safety Assessment
B Safety Risk Management Tracking System
C Preliminary Program Requirements Section 14, ISP & IAP Safety Sections
D Comparative Safety Assessment
E Preliminary Hazard Analysis
F Program Safety Plan
G Final Program Requirements
H Subsystem Hazard Analysis
I System Hazard Analysis
J Operating & Support Hazard Analysis
K System Safety Assessment Report & Safety Requirements Verification Table
L Independent Operational Assessment
M In-Service Review Checklist
N Post-Implementation Safety Assessments
O Post-Implementation Review



Safety Hazard Analyses and Their Relative Position in the Acquisition Management System

Objective

Performing SSE on a program optimizes the safety of a system by identifying, evaluating, and controlling hazards. SSE is also performed to:

- **Comply with FAA orders, the SMS, and AMS direction.** FAA's primary role is to ensure the safety of the NAS. Thus, the agency has issued FAA Order 8040.4, which directs all agency organizations to employ safety risk management in decision making. The safety risk management sections of the FAA SMS Manual present the methodology to comply with the order. Additionally, AMS policy, in accordance with FAA Order 8040.4, requires programs to perform system safety and to report the system safety program status at all decision points and investment reviews. The SRMGSA and the AMS provide more information on this subject.
- **Reduce total cost of development.** SSE reduces safety risk very early in a program's life cycle, thus reducing cost and programmatic risk while also improving system integration and SE overall. This approach also has a positive effect on system performance and the overall schedule. As Figure 31-3 shows, the earlier in the life cycle a problem is found and managed, the easier and less expensive it is to correct.

- **Improve program integration.** Outputs of the system safety process feed other SE processes, which improves the system's overall SE (Figure 31-4).

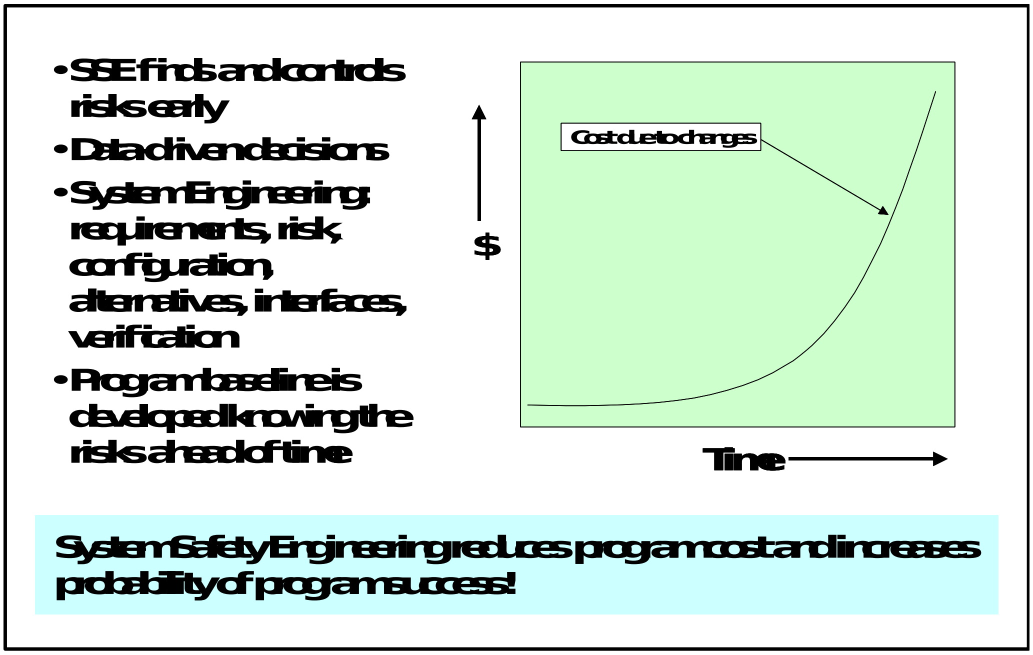


Figure 31-3. Benefits of System Safety Engineering

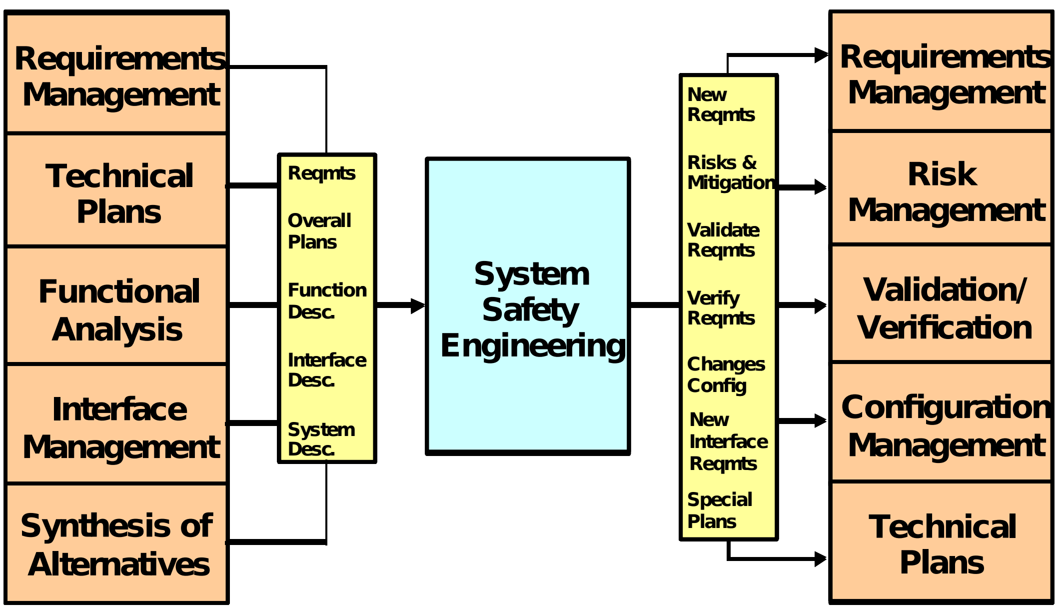


Figure 4.8.1-4. System Safety Engineering's Relationship to Other System Engineering Processes

System Safety Engineering Process Tasks

SSE follows the process tasks outlined in "General Specialty Engineering Process Tasks". These general tasks correlate directly with the specific SSE tasks in Table 31-1 and, as previously stated, appear in the FAA SMS Manual and SRMGSA.

Table 31-1. General Specialty Engineering Tasks Correlated to SSE Tasks

<table>
<tr><th>General Specialty Engineering Process Tasks</th><th>Specific SSE Process Tasks</th></tr>
<tr><td>Obtain or develop an OSED</td><td rowspan="3">Describe the system
• Define scope and objectives
• Define Stakeholders
• Identify criteria and plan for safety risk management effort (including any modeling/simulation potentially required)
• Describe system/change (use, environment and intended function; including future configuration)/current safety issue</td></tr>
<tr><td>Bound the problem and define constraints on the study and design</td></tr>
<tr><td>Select analytical methods and tools</td></tr>
<tr><td rowspan="3">Analyze system parameters to determine system attributes</td><td>Identify hazards
• Use structured approach
• Be comprehensive (and do not dismiss hazards prematurely)
• Employ lessons learned and experience supplemented by checklists</td></tr>
<tr><td>Analyze the risk
• Identify existing mitigations/controls
• Determine risk outcome(s)
• Provide quantitative data (preferred) or qualitative assessments</td></tr>
<tr><td>Assess the risk
• Rank, characterize, and prioritize hazards according to the severity and likelihood of their risk</td></tr>
</table>

<table>
<tr><td>Define and document Specialty Engineering requirements</td><td rowspan="3">Mitigate the risk
• Identify feasible mitigation options
• Develop risk treatment plans
• Define performance targets for each hazard
• Develop a monitoring plan
• Implement and verify the implementation of mitigations
• Record, monitor, and track to completion of monitoring plan
• Verify predicted residual risk</td></tr>
<tr><td>Coordinate results with stakeholders</td></tr>
<tr><td>Document the Specialty Engineering analysis in a Safety Risk Management Document (SRMD)</td></tr>
</table>

System Safety Engineering Outputs and Products

The following products are SSE outputs.

Program Planning

Per the SRMGSA, each program has to have a Program Safety Plan (PSP) which is the overall plan for conducting system safety management in the AMS. It is recommended that individual programs, when developing a program-specific PSP, consult the SRMGSA, which also develops the requirements for the program vendor's or contractor's System Safety Program Plan (SSPP).

Analysis Products

Table 31-2 lists the Safety Risk Management (SRM) products done within the AMS and where further information will be found.

Table 31-2. Products of System Safety Engineering

System Safety Process Products	How To Reference
Research and Systems Analysis phase (RSA)	SRMGSA sections on the RSA phase safety products
Operational Safety Assessment (OSA)	SRMGSA
Comparative Safety Assessment (CSA)	SRMGSA

Preliminary Hazard Analysis (PHA) {*for AMS-related assessments*}	SRMGSA
Hazard Analysis Worksheet (HAW) {*for operations-related assessments*}	SRMGSA
Program Safety Plan (PSP)	SRMGSA
System Safety Program Plan (SSPP)	SRMGSA
Subsystem Hazard Analysis (SSHA)	SRMGSA

Table 31-2. Products of System Safety Engineering—Continued

System Safety Process Products	How To Reference
System Hazard Analysis (SHA)	SRMGSA
Operating and Support Hazard Analysis (O&SHA)	SRMGSA
System Safety Assessment Report (SSAR)	SRMGSA
Safety Risk Management Tracking System (SRMTS)	SMS Manual SRMGSA
Safety Requirements Verification Table (SRVT)	SRMGSA

This page intentionally left blank.

32 – Hazardous Materials Management/ Environmental Engineering

Introduction

Hazardous Materials Management/Environmental Engineering (HMM/EE) is the subset of Specialty Engineering concerned with the impacts both of the program on the environment and of the environment on the program. Federal, state, and local environmental agencies have established mandates that regulate program impacts on the environment. These mandates include requirements to manage hazardous materials and to safeguard natural resources including ambient air, water, and land-based resources. FAA orders and directives (e.g., FAA Order 1050.10C, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities) relate federal environmental regulations to FAA activities and also provide additional environmental requirements specific to NAS operations. Conversely, environmental impacts on programs vary, depending on site-specific environmental conditions that may affect FAA operational requirements. The following sections describe the purpose and general process of HMM/EE within systems engineering (SE).

Definition

HMM/EE is the mechanism applied within the SE process to ensure a program's ongoing compliance with applicable environmental laws. Compliance with various environmental regulations is required throughout a program's life cycle, requiring early and continuous application of HMM/EE principles. Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. Through HMM/EE, the breadth of environmental requirements are continuously monitored and considered to ensure that FAA's programs take the steps to maintain compliance.

Additional issues concerning the applicability of state and local agency requirements to federal agencies are to be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications. For example, the Resource Conservation and Recovery Act establishes standards for managing and disposing of hazardous wastes that result from various processes during program operation, and at the end of the program's life cycle. These requirements may be administered through state agencies.

HMM/EE is also the SE process designed to provide early, pre-deployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. HMM/EE processes highlight the impacts that environmental conditions and site-specific characteristics may have on a program. FAA specifications are the primary tool developed for various types of equipment to delineate operating conditions that shall be considered during the program's developmental stages. For example, the general FAA specification for electronic equipment, FAA-G-2100, details the design standards that shall be followed to ensure equipment functionality in environmental conditions of both seismic zones and temperature extremes. HMM/EE verifies that similar standards are considered and followed in the SE process to ensure the reliability of systems fielded under unique environmental settings.

Objective

HMM/EE is performed to:

- Support reliable, safe, and sustained NAS operations;
- Ensure compliance with FAA, federal, state, and local environmental requirements;
- Ensure environmental considerations are included in the acquisition management process;
- Track the status of environmental issues with new and existing systems; and
- Minimize cost and schedule risks through early detection of environmental issues.

Through various regulations, such as FAA Order 1050.17, Airway Facilities Environmental and Safety Compliance Program, FAA has mandated and set requirements to comply with applicable environmental regulations. The FAA Acquisition Toolset System (FAST) ensures that these regulations are considered in the acquisition process in AMS Section 4.8, Environmental, Occupational Safety and Health, and Energy Considerations.

FAA investment programs are subject to federal environmental, occupational safety and health, and energy management statutes; regulations; executive orders; and Presidential memoranda. Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. Additional issues concerning how state and local agency requirements apply to federal agencies should be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications.

Service organizations must understand the national concern and sensitivity of these issues and address them in program planning and execution.

The following illustrate some of the requirements:

- The Clean Air Act (CAA) established a comprehensive program for protecting and enhancing the nation's air quality and stratospheric ozone layer. State air pollution prevention agencies have developed emission control strategies and permit programs, particularly for new construction or modifications of sources of air pollution. The CAA also established the National Emission Standards for Hazardous Air Pollutants (NESHAP) requiring permitting and implementation of pollution control standards for certain air pollutants.
- The Clean Water Act (CWA) established the National Pollutant Discharge Elimination System (NPDES), which controls water pollution by regulating point sources that discharge pollutants into the waters of the United States. At ATO facilities, cooling tower discharges, boiler blowdown and/or other thermal discharges to waters of the United States may require an NPDES permit. Additionally, stormwater discharges resulting from ATO construction activities may require an NPDES permit.
- ATO installs and maintains thousands of NAS facilities across the United States and therefore must consider the impact these installations could have on culturally significant sites. Cultural resources include, but are not limited to historic properties (as listed in or eligible for the National Register of Historic Places), Native American graves and cultural items, and archeological sites. Cultural resource management refers to the legally mandated protection of these resources.
- The National Environmental Policy Act "requires preparation of an environmental assessment or an environmental impact statement for all proposed federal actions that are not categorically excluded. Depending on the results, an environmental assessment can lead to an environmental impact statement or a finding of no significant impact. Following the prescribed review periods, FAA may make a decision on the federal action."
- The Occupational Safety and Health Administration (OSHA) "requires a safe and healthful workplace for all employees, and compliance with OSHA standards."
  For Example: OSHA (29 CFR §1910.38) and GSA (Federal Property Management Regulations) require the FAA to establish and maintain an Occupant Emergency Plan for all FAA facilities. In the event an acquisition program impacts egress routes or fire safety of a facility,

the plan must be updated by the program office or the Product Team performing the project.

- The Energy Policy Act of 2005, the Energy Independence and Security Act of 2007, and related Executive Orders (Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management, and Executive order 13514, Federal Leadership in Environmental, Energy, and Economic Performance) established energy and water efficiency requirements for the federal government. Additionally, the Guiding Principles for Federal Leadership in High Performance and Sustainable Buildings commits FAA to a common set of sustainable principles for integrated design, energy performance, and water conservation.
- The Resource Conservation and Recovery Act (RCRA) is the primary federal statute regulating the management and disposal of hazardous wastes. ATO facilities must manage hazardous wastes in accordance with the requirements of both federal and state-specific programs to ensure compliance and proper management of the wastes. FAA is exposed to “cradle-to-grave” liability for hazardous wastes. Proper management and disposal will minimize the agency’s exposure to this liability.

Environmental, safety and health, and energy conservation considerations apply from the beginning of the life cycle management process through product disposal. The acquisition program baseline will incorporate estimates for the full cost of complying and allow sufficient time for doing so. FAST contains procedural guidance for required actions.

When applied early, HMM/EE identifies applicable environmental requirements to include in the development and acquisition of new systems, thereby providing significant savings through risk mitigation, cost avoidance, and enhancement of system efficiency. Additionally, consideration of environmental impacts on systems while they are in the developmental stages ensures their functionality in various field conditions.

When applied as part of in-service program management, HMM/EE analyzes the impact that engineering changes in the field may have on environmental concerns. Additionally, HMM/EE evaluates the impact that regulatory changes may have on currently fielded systems.

At the end of program life cycle, HMM/EE ensures compliance with applicable environmental requirements during decommissioning and disposition. As obsolete equipment is removed, HMM/EE ensures that replacement equipment complies with applicable environmental regulations. Further,

decommissioning and removal of obsolete equipment require HMM/EE considerations to ensure that the final disposition/disposal of obsolete equipment also is conducted in accordance with applicable environmental requirements.

Programs that fail to fully incorporate HMM/EE principles may have significant impacts on NAS operations. Noncompliant programs may:

- Be removed from service through regulatory enforcement actions;
- Require costly post-fielding/retrofit modifications; or
- Incur fines.

Additionally, costs associated with new equipment fielding, and obsolete equipment disposition and disposal may lead to significant budgeting issues if they are not considered during the program development phase.

HMM/EE Outputs and Products

Throughout the various phases of the system acquisition process, HMM/EE is used in developing and reviewing key documents. Early implementation of HMM/EE principles minimizes the impact that environmental requirements may have on system costs and operations. During the preliminary activities, such as development of mission needs, requirements, and investment analysis, HMM/EE is used to make initial assumptions and estimates on how environmental considerations may come into play throughout the various life cycle stages.

During the solution implementation phase of the acquisition process, HMM/EE is used to shape portions of the statement of work (SOW) and system specifications documents as they relate to environmental considerations. For example, SOWs may be developed to support FAA efforts to meet National Environmental Policy Act demands that federal agencies consider environmental impacts as part of proposed federal actions for federal building energy efficiency performance standards.

During the in-service management phase of the system life cycle, HMM/EE is used to address issues that may arise unexpectedly in the field. In particular, older pieces of equipment that may not have been developed with HMM/EE in mind may require corrective measures to meet environmental regulations. Additionally, the set of ever-changing environmental regulations may impact the way systems are operated. Finally, as old systems are decommissioned, HMM/EE is necessary to ensure that all disposal actions consider applicable environmental laws.

Program Integration

As part of the SE process, HMM/EE provides expertise for developing various documents required for program integration. Throughout the various life cycle phases, HMM/EE ensures that all applicable regulations and environmental conditions are properly addressed so that their impacts are addressed appropriately. For example, HMM/EE would support development of the IRD, keeping in mind environmental regulations that require federal agencies to verify that their activities do not negatively impact certain ecosystems. Similarly, HMM/EE's role in developing Integrated Program Plans, SOWs, Disposition/Disposal Plans, and other such documents generates comments and input concerning compliance requirements. that the requirements may impact the progress of program implementation, and FAA's compliance status and future liabilities.

Included in the HMM/EE aspects of program integration is a functional analysis of the OSED (see Chapter 12 (Functional and Performance Allocation)). This portion of the functional analysis ensures that the environmental conditions that the various systems face are fully considered and that plans are appropriately developed to address identified conditions. Figure 32-1 below depicts HMM/EE Inputs and Outputs.

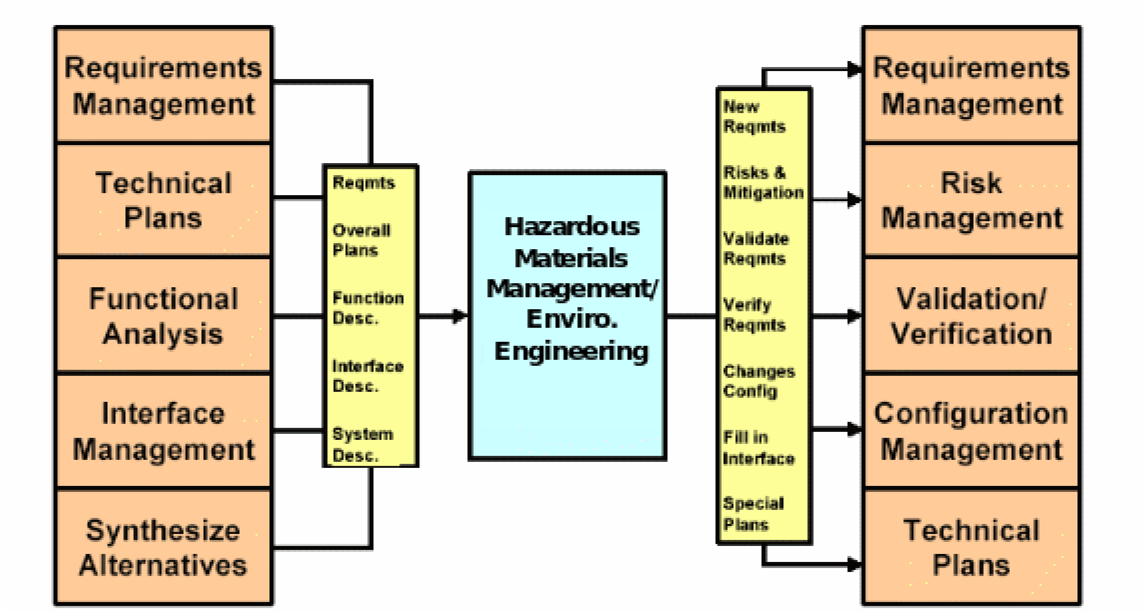


Figure 32-1. HMM/EE's Relationship to Other Systems Engineering Processes

Program Planning

FAA Order 1050.17, Airway Facilities Environmental Compliance Program, implements the overall program for environmental compliance at FAA facilities. Each region in the agency has an Environmental Compliance Plan

(ECP). The ECP is designed to identify and address compliance requirements in 19 environmental areas for all facilities, and therefore all systems within a region.

In addition, FAA Order 4600.27A, Personal Property Management, and AMS Section 2.7, In-Service Management, provide the requirements and framework for developing and implementing system-specific disposal plans for obsolete systems. These disposal plans are part of the Integrated Program Plan appendices; see Chapter 3, Integrated Technical Planning Process.

Products

Additionally, the Hazardous Materials Management/Environmental Engineering process, must provide a program the capability to produce an inventory of the hazardous materials that fielded equipment may contain. This information has many purposes, including, but not limited to:

- Ensuring protection of the environment and surrounding communities;
- Ensuring regulatory compliance during the program's operational life;
- Supporting the safety of personnel working with equipment; and
- Supporting disposition/disposal efforts when obsolete equipment is removed from service.

References

Airway Facilities Environmental and Safety Compliance Program. FAA Order 1050.17. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

Energy and Water Management Program for FAA Buildings and Facilities. FAA Order 1053.1A. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

In-Service Management. FAA Acquisition Management System, Section 2.7. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC. http://fast.faa.gov/.

Personal Property Management. FAA Order 4600.27A. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities. FAA Order 1050.10C. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

National Environmental Policy Act (NEPA) Implementing Instructions for Airport Projects. FAA Order 5050.4B. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management.

Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance.

Energy Independence and Security Act of 2007.

Energy Policy Act of 2005.

Occupational Safety and Health Act of 1970, and the implementing regulations at 29 CFR 1910, 29CFR 1926 and 29 CFR 1960.